RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: NCS-R05

DNS DoS: Recent Vulnerabilities and Modern Defenses

Dr. Huayi Duan
Senior Postdoctoral Researcher
Network Security Group
ETH Zürich

Jelte van Bommel
Research Scientist
Network Security Group
ETH Zürich

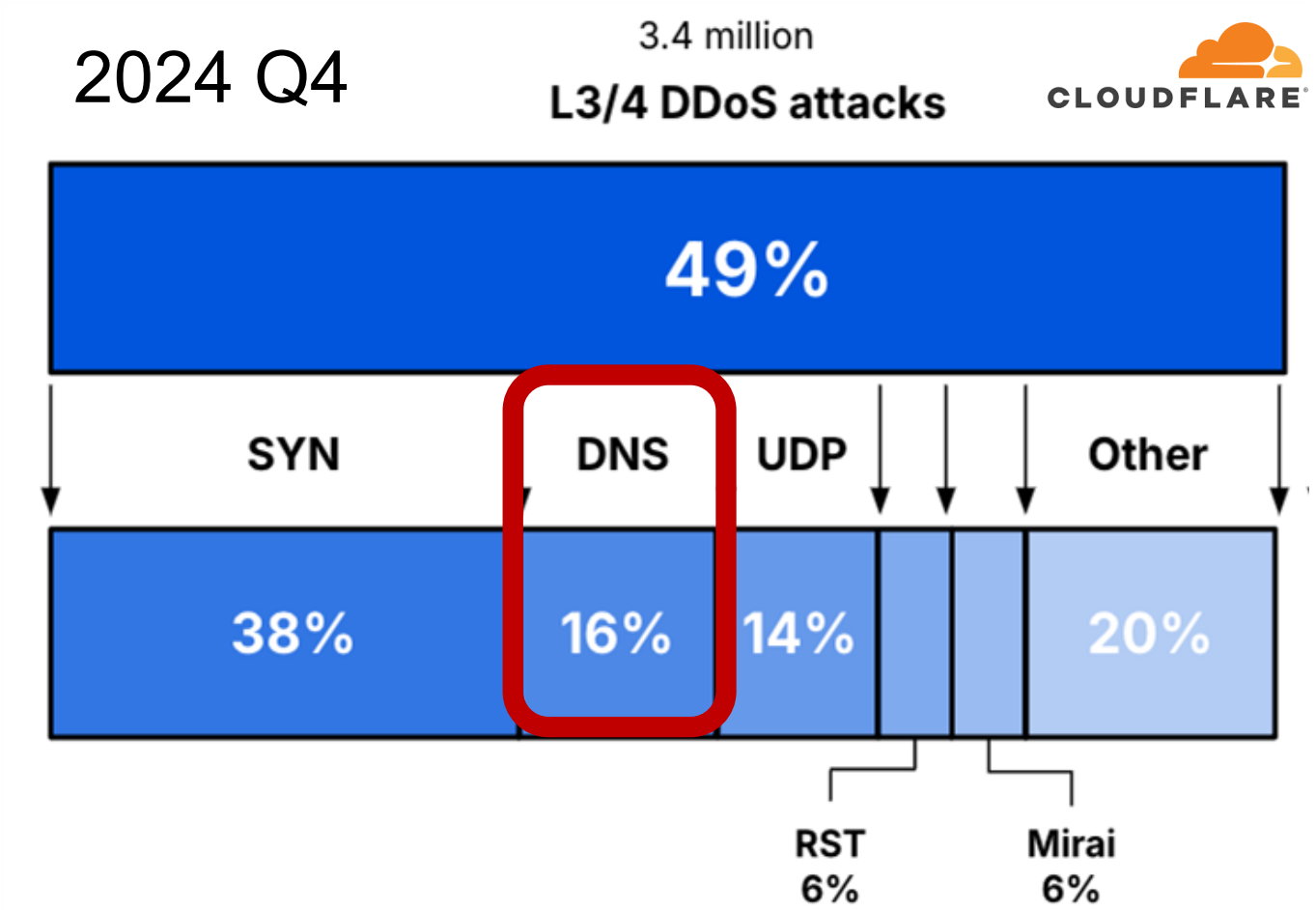
Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

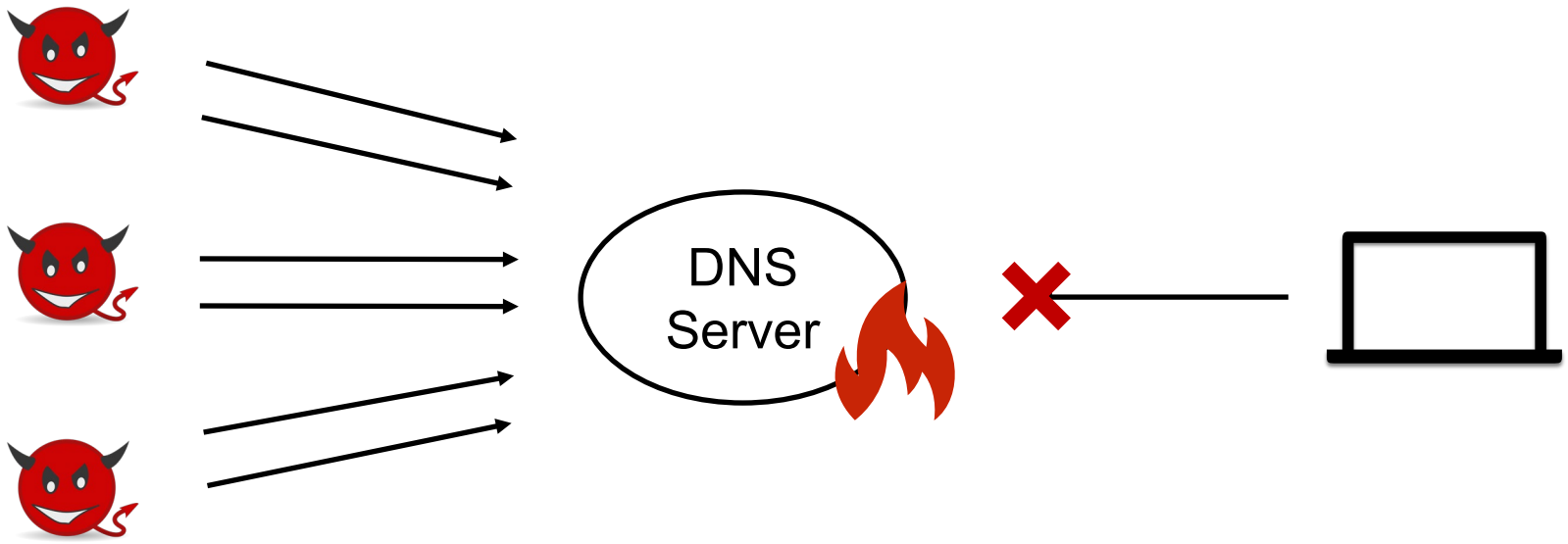
DNS remains a major target for DoS



Source: https://blog.cloudflare.com/ddos-threat-report-for-2024-q4/

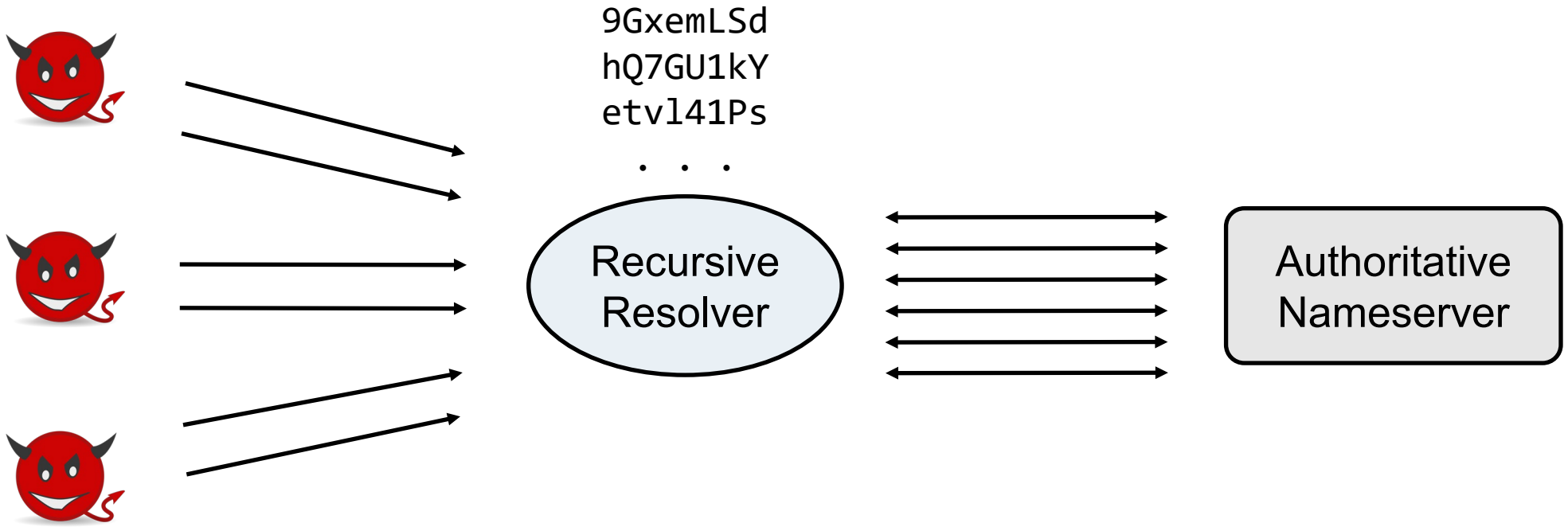
Evolution of DoS attacks against DNS

Conventional distributed flooding



Evolution of DoS attacks against DNS

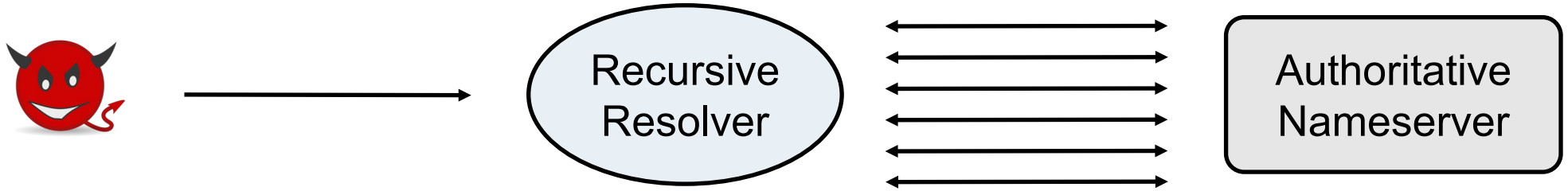
Pseudo-random subdomain (PRSD) to bypass resolver cache



Evolution of DoS attacks against DNS

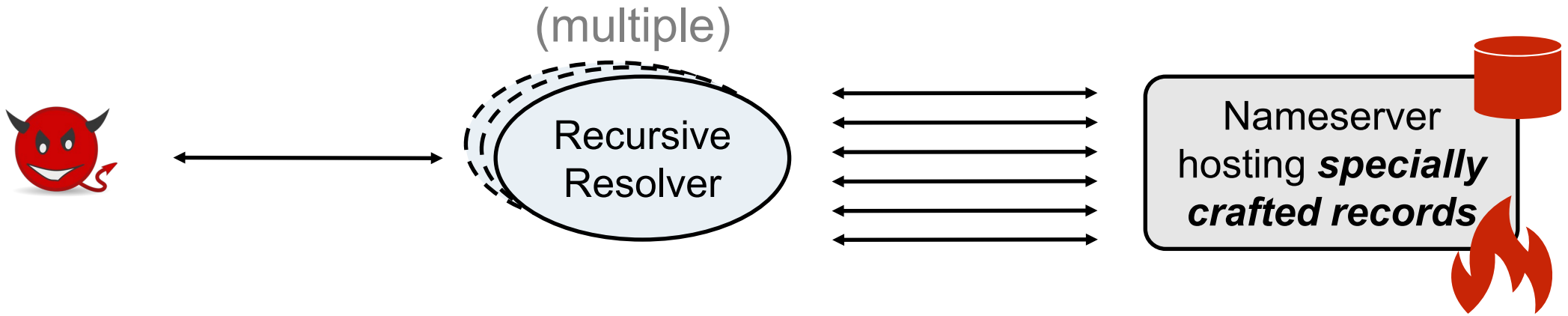
Self-amplification: each request triggers excessive work on servers

distinct from **reflection-amplification**



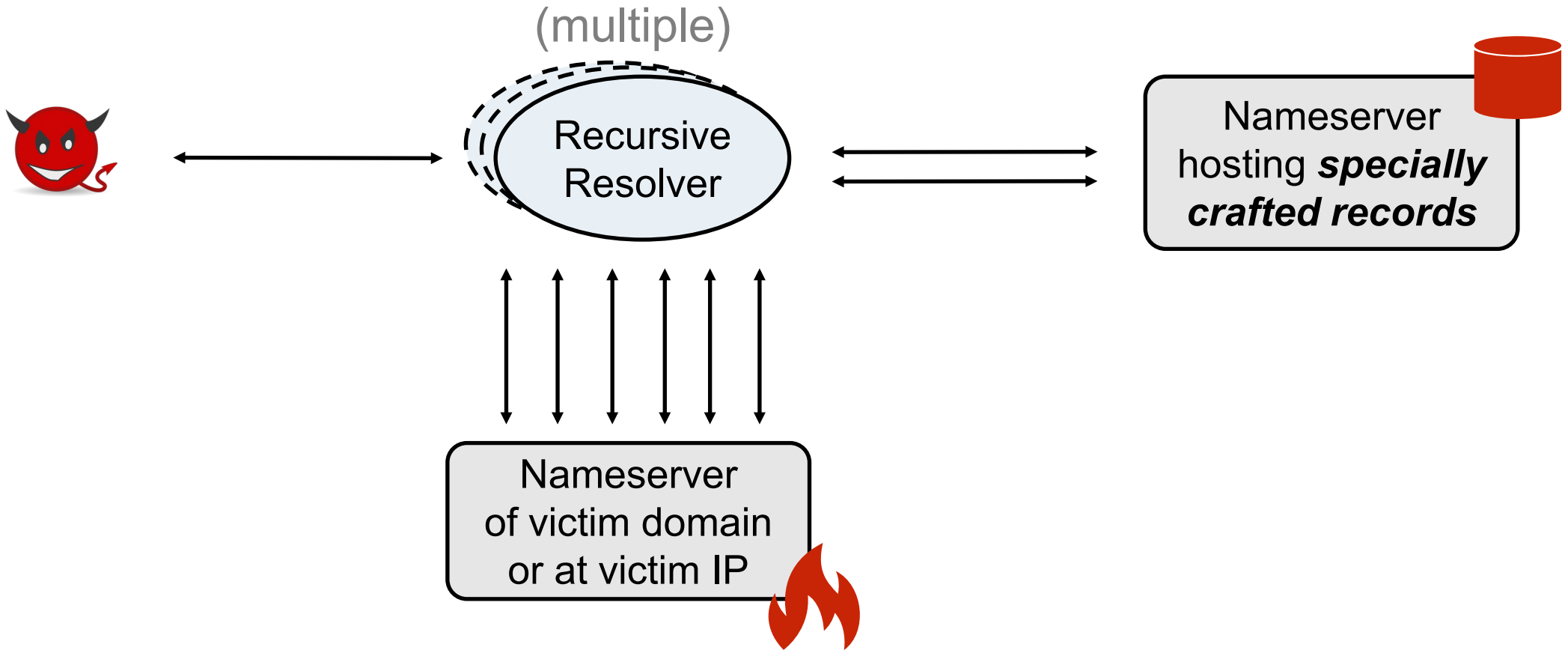
Self-amplification overview

Possible target: nameserver where attacker can set up DNS zones



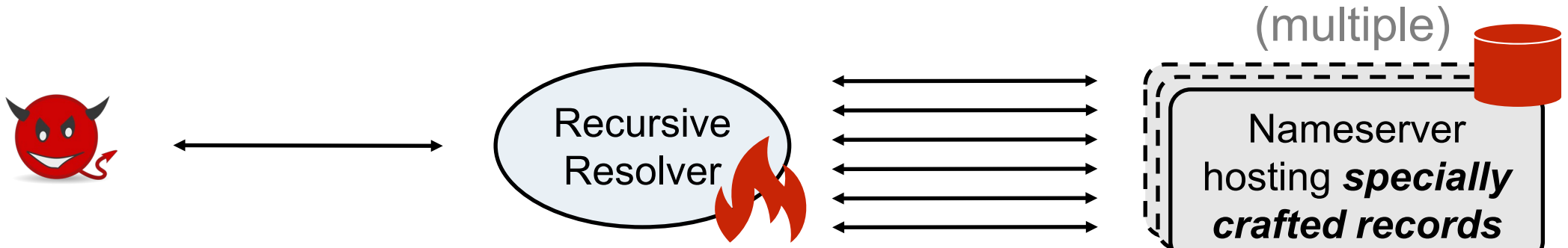
Self-amplification overview

Possible target: nameserver pointed by malicious delegation records


(multiple)
Recursive Resolver
Nameserver hosting ***specially crafted records***
Nameserver of victim domain or at victim IP

Self-amplification overview

Possible target: recursive resolver accessible to attacker



QPS = 30
(queries per second)

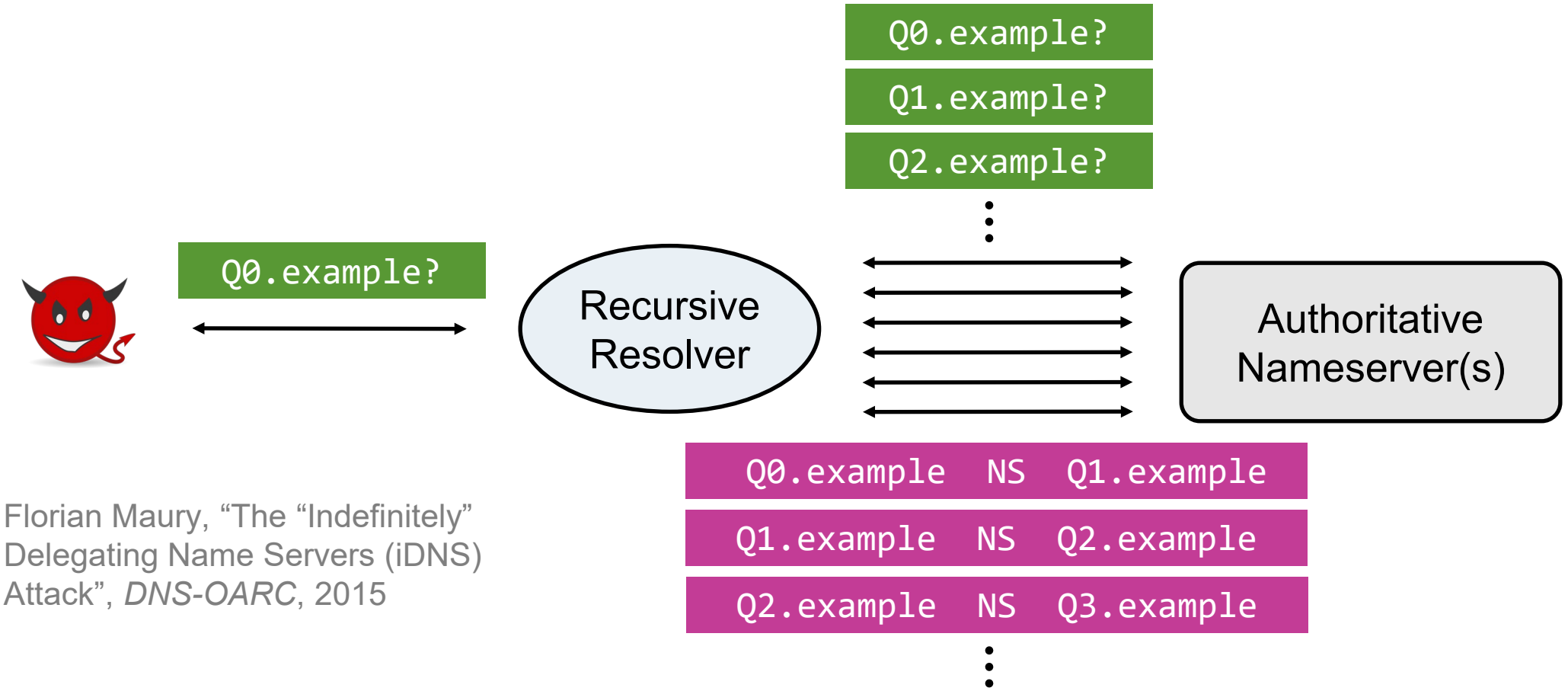
8 CPUs
32GB RAM

MAF = 500
(message amplification factor)

Attack impact: degrade a production-grade resolver's ability to serve legitimate client queries by **~50%**, comparable to PRSD attack with **~21K QPS**.

Self-amplification variants

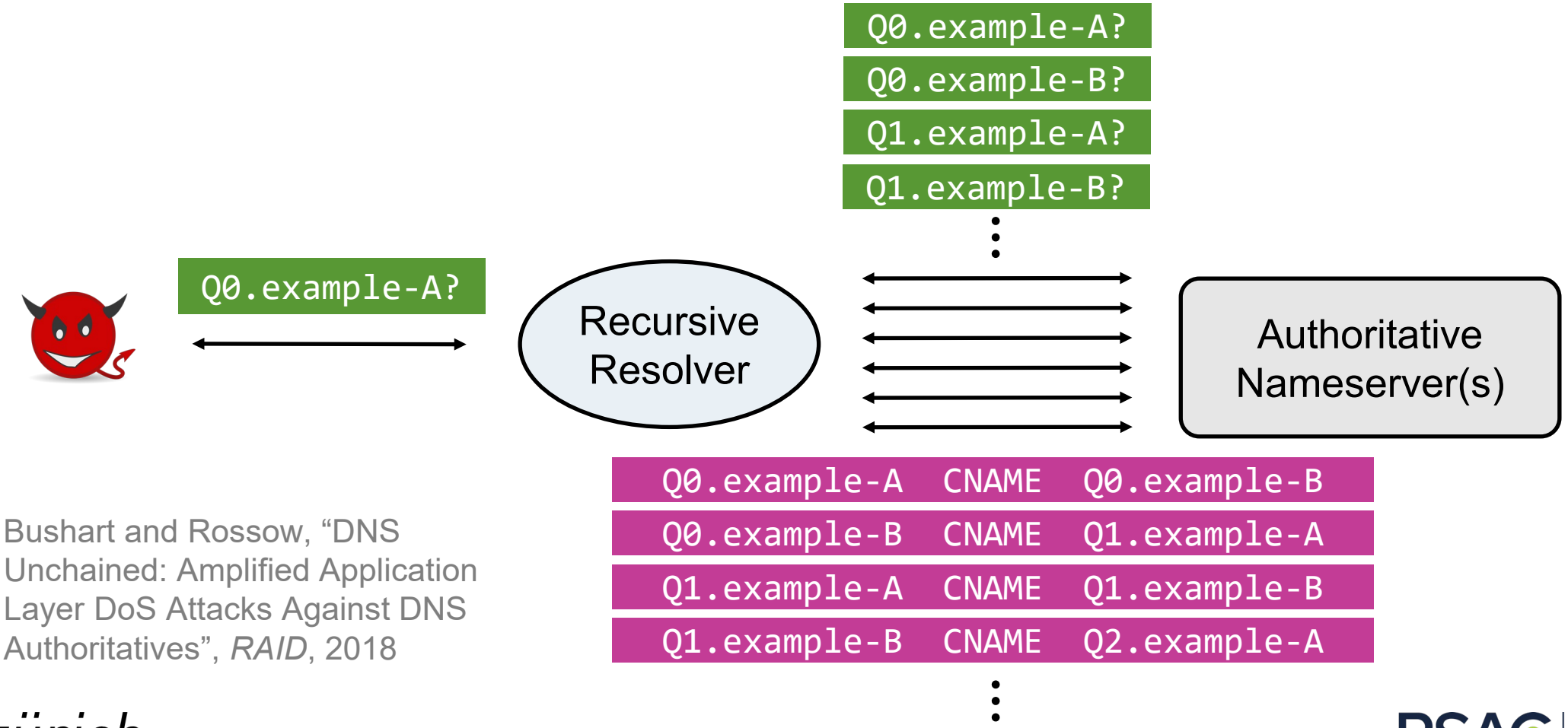
iDNS attack [1]: cascading delegation records



[1] Florian Maury, "The "Indefinitely" Delegating Name Servers (iDNS) Attack", *DNS-OARC*, 2015

Self-amplification variants

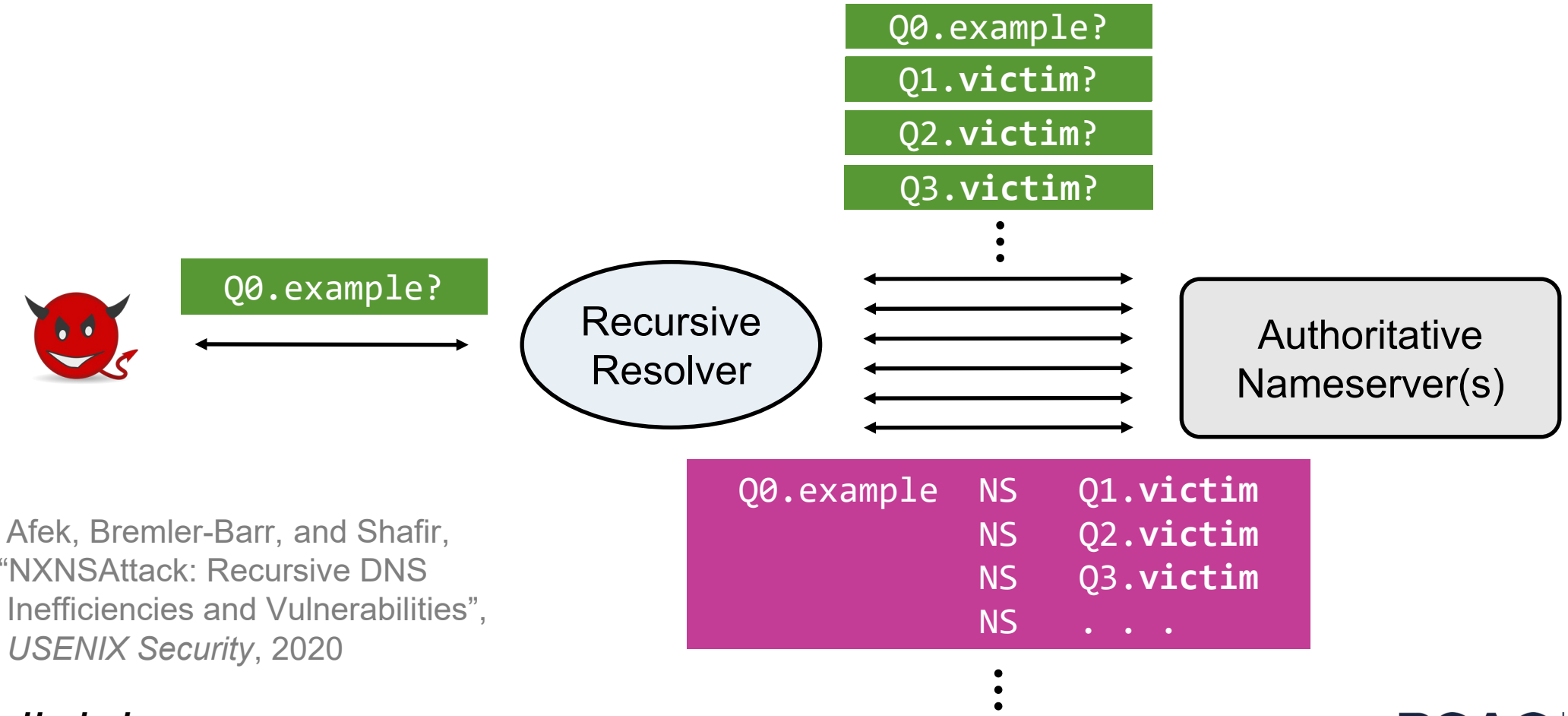
Unchained attack [2]: alternating CNAME chain



[2] Bushart and Rossow, "DNS Unchained: Amplified Application Layer DoS Attacks Against DNS Authoritatives", *RAID*, 2018

Self-amplification variants

NXNSAttack [3]: proactive and parallel fetching of nameservers



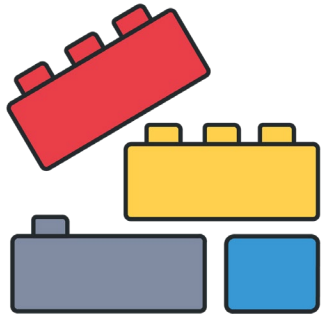
[3] Afek, Bremler-Barr, and Shafir, "NXNSAttack: Recursive DNS Inefficiencies and Vulnerabilities", *USENIX Security*, 2020

Systematization of DNS self-amplification

How many such vulnerabilities exist?

What is the maximum achievable amplification effect?

Identify ***amplification primitives*** → Establish their ***composability***



⋮

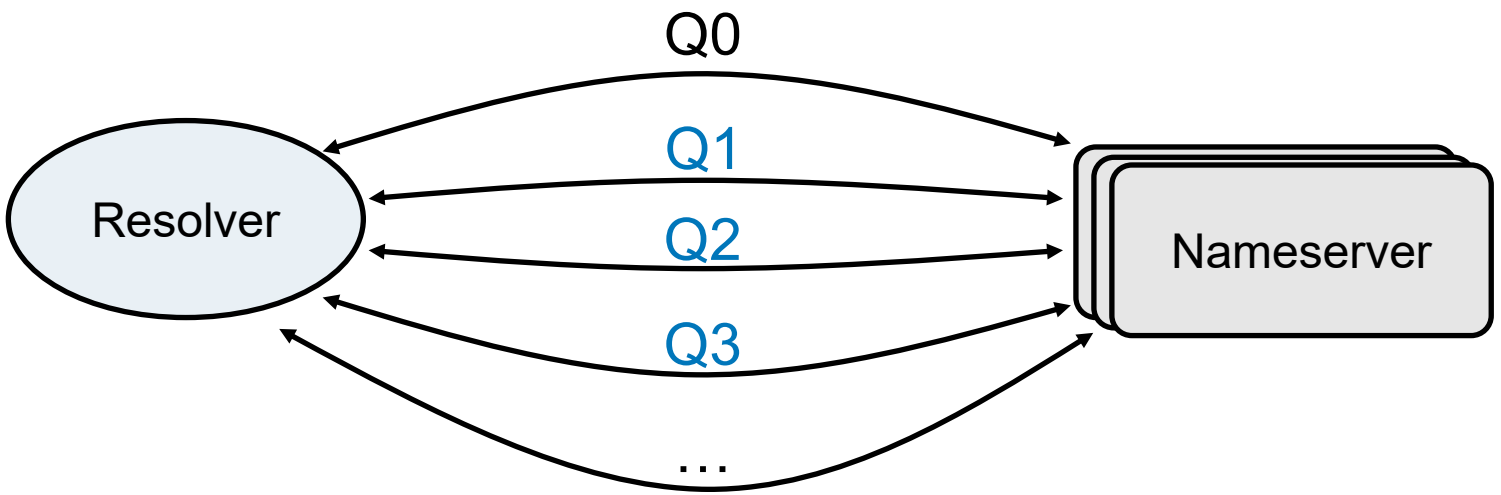
CAMP [4]
(compositional amplification)

[4] Duan, Bearzi, Vieli, Basin, Perrig, Liu, and Tellenbach, "CAMP: Compositional Amplification Attacks against DNS", *USENIX Security*, 2024

Taxonomy of amplification primitives

Names queried in amplified resolution

Base Q0 → {Q1, Q2, Q3, …} ***Derivatives***



Taxonomy of amplification primitives

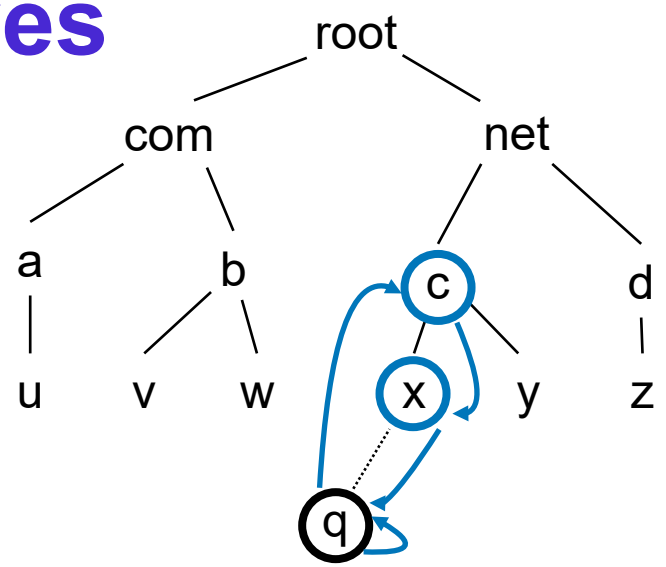
Names queried in amplified resolution

Base Q0 → {Q1, Q2, Q3, …} ***Derivatives***

Names on the same path?

All

Self-probing



Taxonomy of amplification primitives

Names queried in amplified resolution

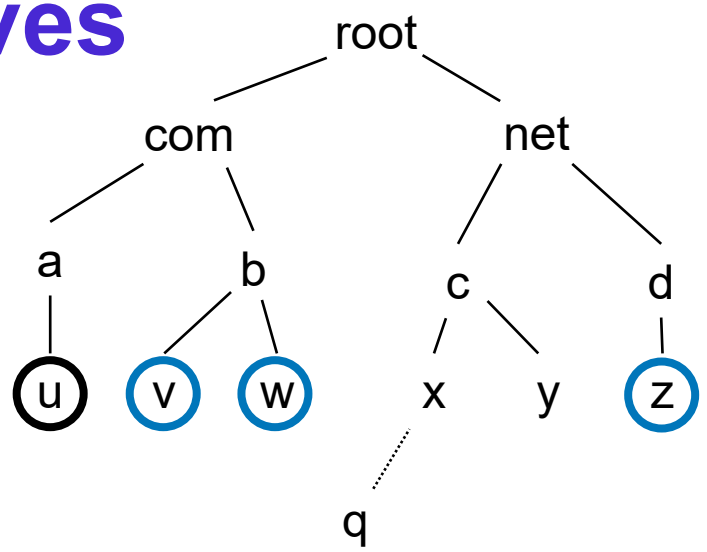
Base Q0 → {Q1, Q2, Q3, …} ***Derivatives***

Names on the same path?

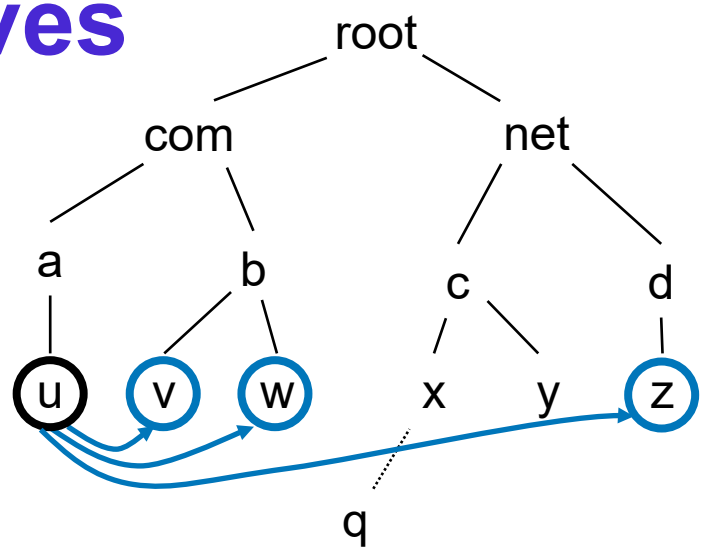
All

None

Self-probing



Taxonomy of amplification primitives



Names queried in amplified resolution

Base Q0 → {Q1, Q2, Q3, …} ***Derivatives***

Names on the same path?

All

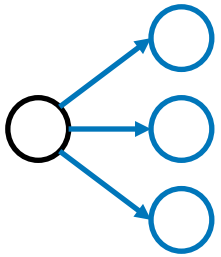
Self-probing

None

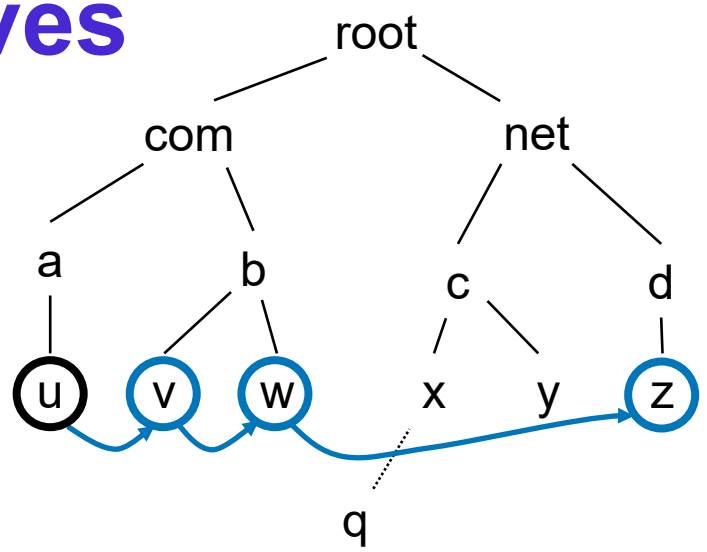
Independent derivatives?

Yes

Fan-out



Taxonomy of amplification primitives



Names queried in amplified resolution

Base Q0 → {Q1, Q2, Q3, …} ***Derivatives***

Names on the same path?

All

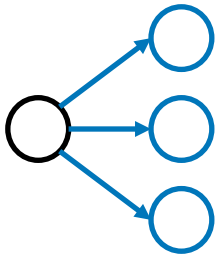
Self-probing

None

Independent derivatives?

Yes

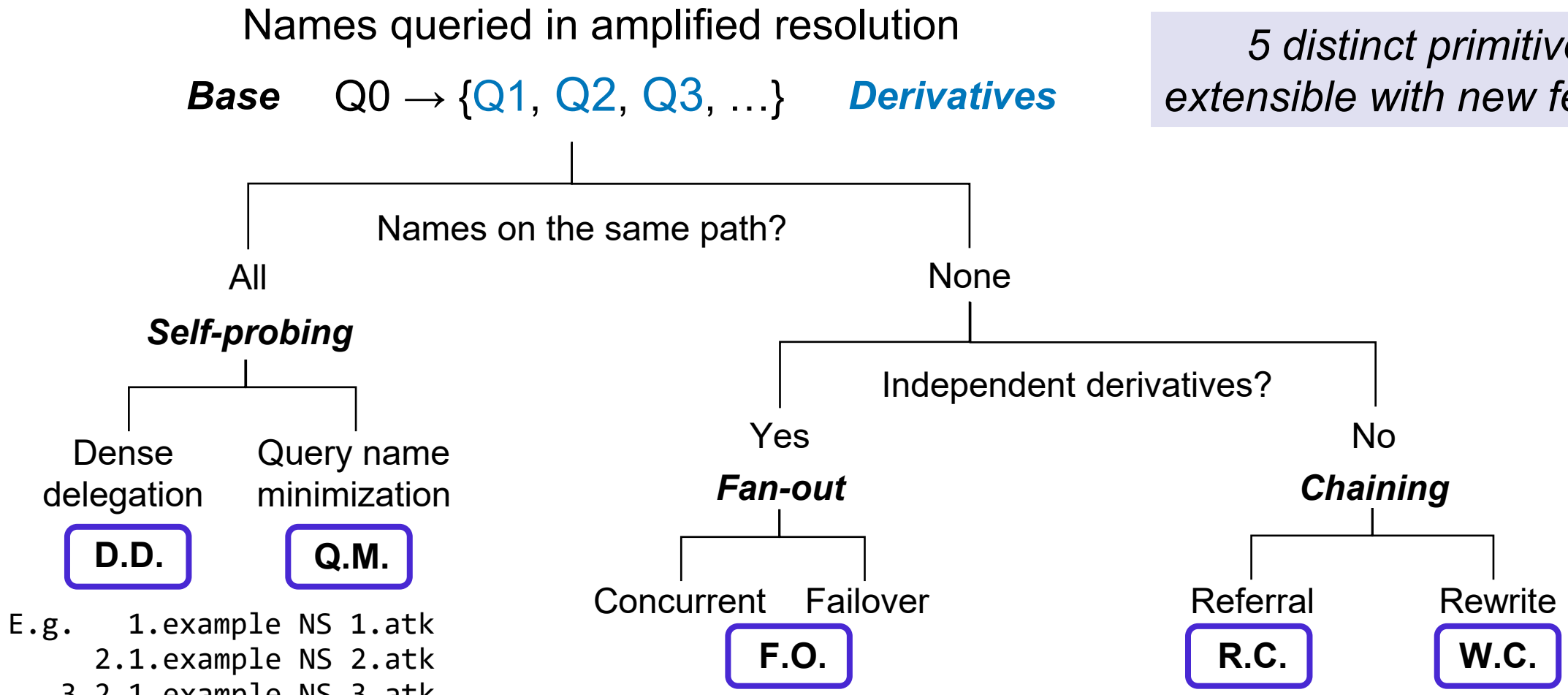
Fan-out



No

Chaining

Taxonomy of amplification primitives



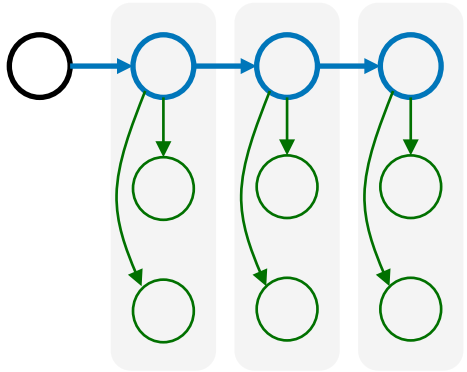
5 distinct primitives, extensible with new features

Composability analysis

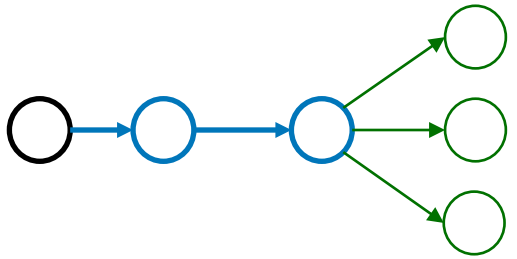
Observation: one primitive's derivative can be another primitive's base

primary ***secondary***

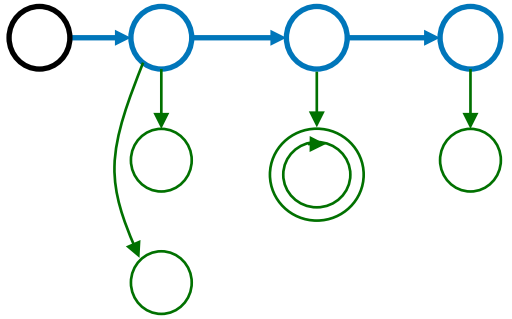
Focus on ***regular multiplicative*** compositions



additive



irregular



Composability analysis

Results: 16/25 regular multiplicative compositions

Compo-sability		Secondary				
		F.O.	R.C.	W.C.	Q.M.	D.D.
Primary	F.O.	✓	✓	✓	✓	✓
	R.C.	✗	✗	✗	✓	✓
	W.C.	✓	✓	✗	✓	✓
	Q.M.	✗	✗	✗	✗	✗
	D.D.	✓	✓	✓	✓	✓

Composability analysis

Results: 16/25 regular multiplicative compositions

Compo-sability		Secondary				
		F.O.	R.C.	W.C.	Q.M.	D.D.
Primary	F.O.	✓	✓	✓	✓	✓
	R.C.	✗	✗	✗	✓	✓
	W.C.	✓	✓	✗	✓	✓
	Q.M.	✗	✗	✗	✗	✗
	D.D.	✓	✓	✓	✓	✓

All permitted (implicitly) by RFCs, except two

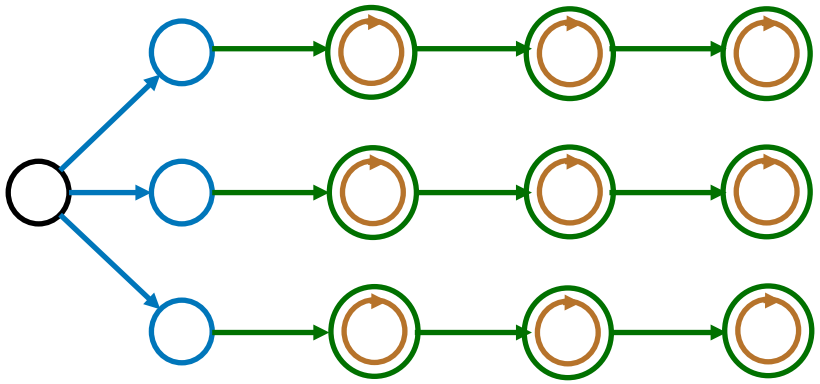
> The domain name used as the value of an NS record, or part of the value of an MX record **must not be an alias.**
>
> – RFC2181

Still allowed by many resolvers…

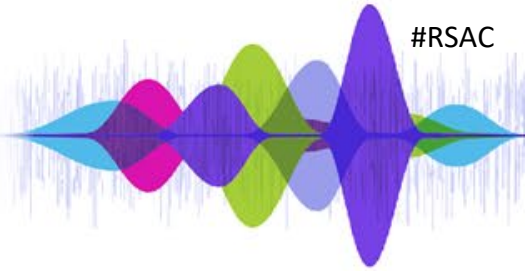
Composability analysis

Exponentially many ***multi-dimensional*** (regular or not) compositions!

Example: **Fan-out** X **Chain** X **Self-probing**



Evaluation on resolvers (before patching)



Resolver #1

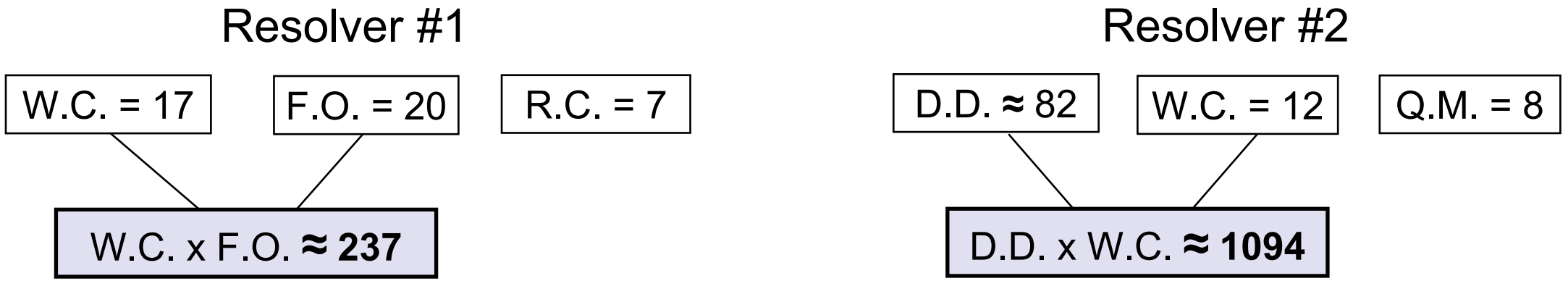
W.C. = 17 | F.O. = 20 | R.C. = 7

Resolver #2

D.D. ≈ 82 | W.C. = 12 | Q.M. = 8

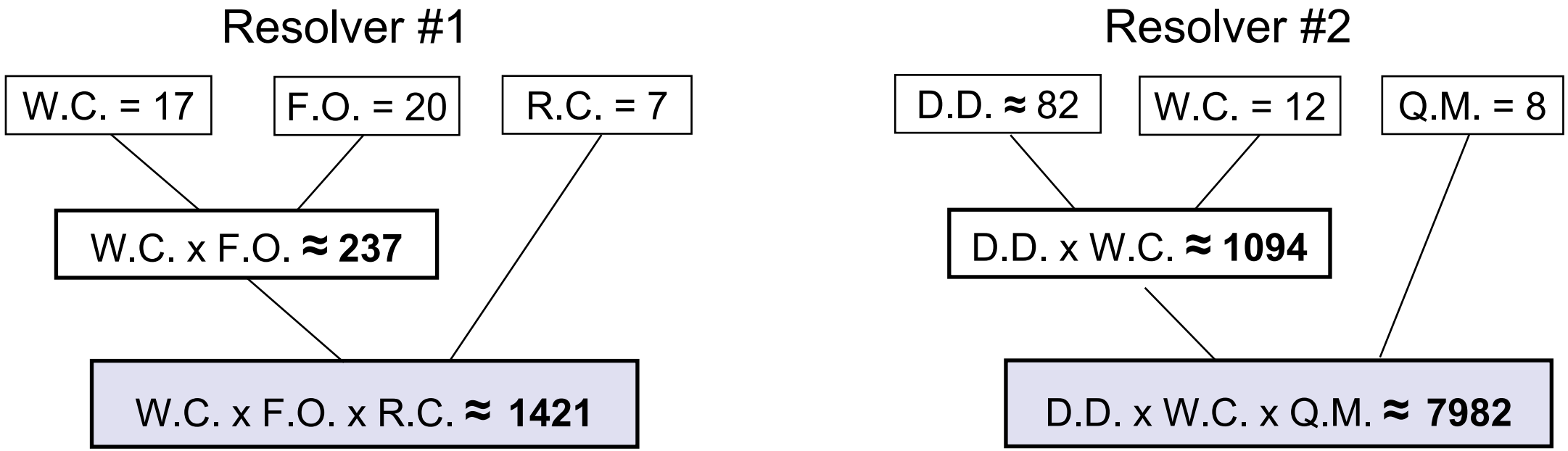
MAFs of amplification primitives are reasonably limited

Evaluation on resolvers (before patching)



CAMP can bypass query limits on individual features

Evaluation on resolvers (before patching)



CAMP effect can grow exponentially in #dimensions

Now many resolvers have max MAF < 100

Remarks on self-amplification

- **Inherent** to the design of DNS
- Some resulted from **ambiguities** in protocol specifications
- **Systematic** analysis & mitigation is necessary

> The recommended priorities for the resolver designer are:
>
> 1. Bound the amount of work (packets sent, parallel processes started) so that a request can't get into an infinite loop or start off a chain reaction of requests or queries with other implementations EVEN IF SOMEONE HAS INCORRECTLY CONFIGURED SOME DATA.
>
> – RFC1034

RSAC | 2025 Conference

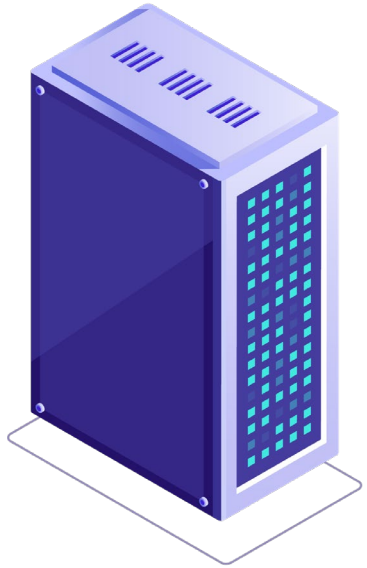
How can we defend DNS infrastructure against DoS attacks?

Monitoring

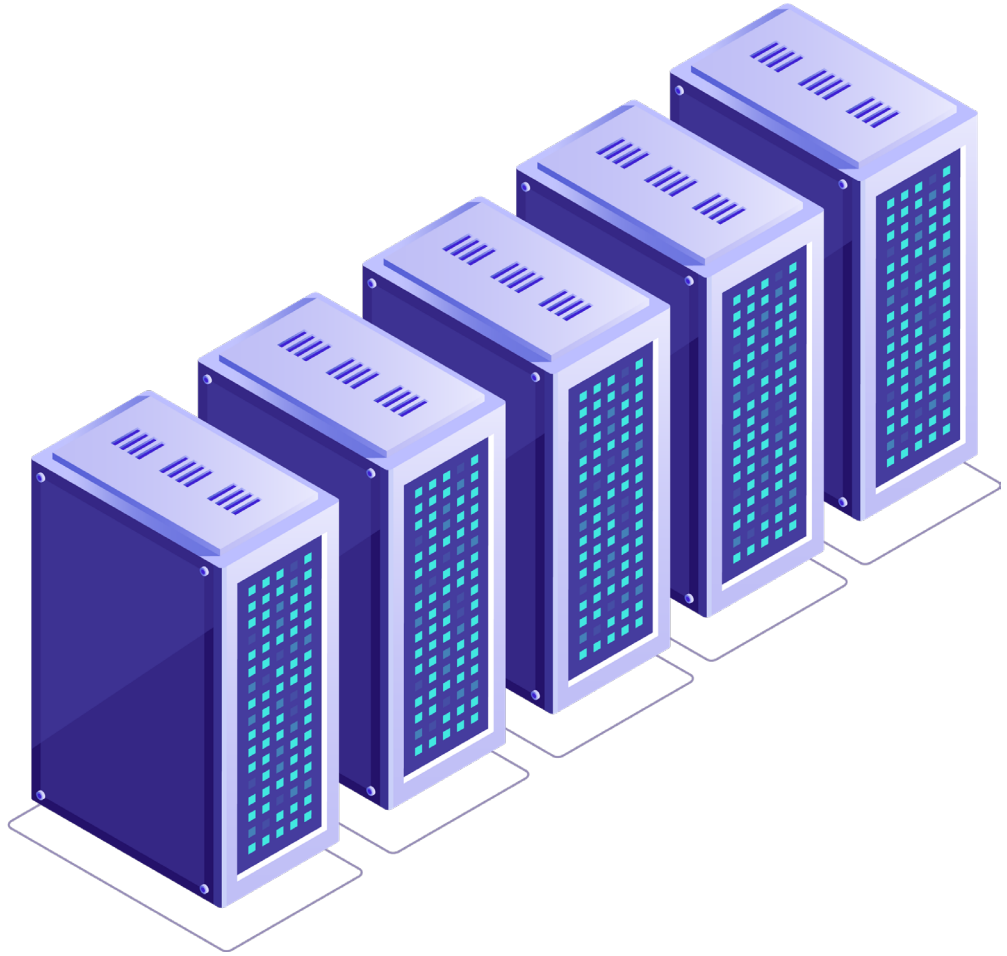
- Availability, correctness, latency, queries per second, query distributions
- Anomaly-based filtering (e.g., [5])

[5] Bushart and Rossow, “Anomaly-based Filtering of Application-Layer DDoS Against DNS Authoritatives”, *EuroS&P*, 2023

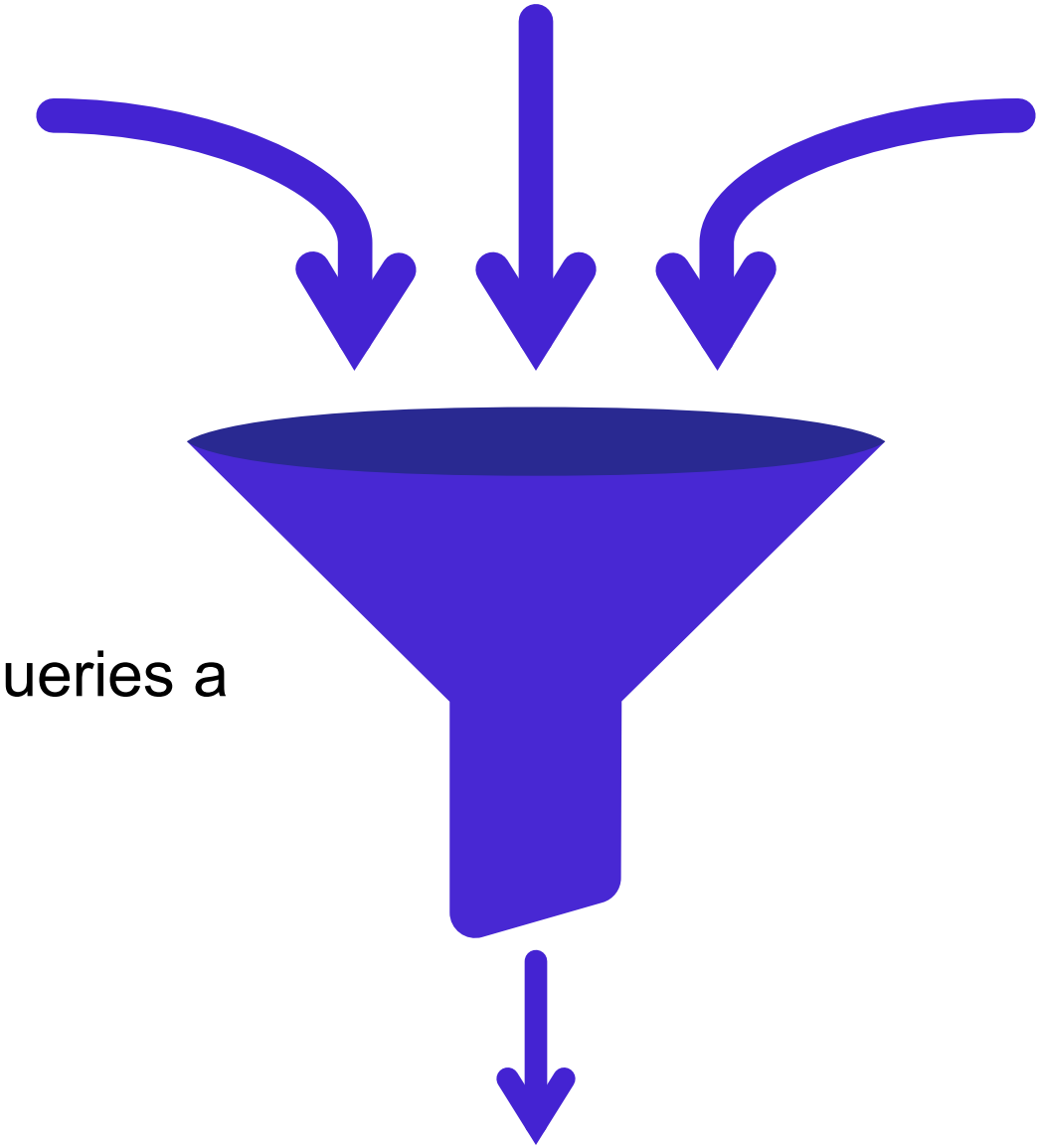
Overprovisioning



10x – 100x

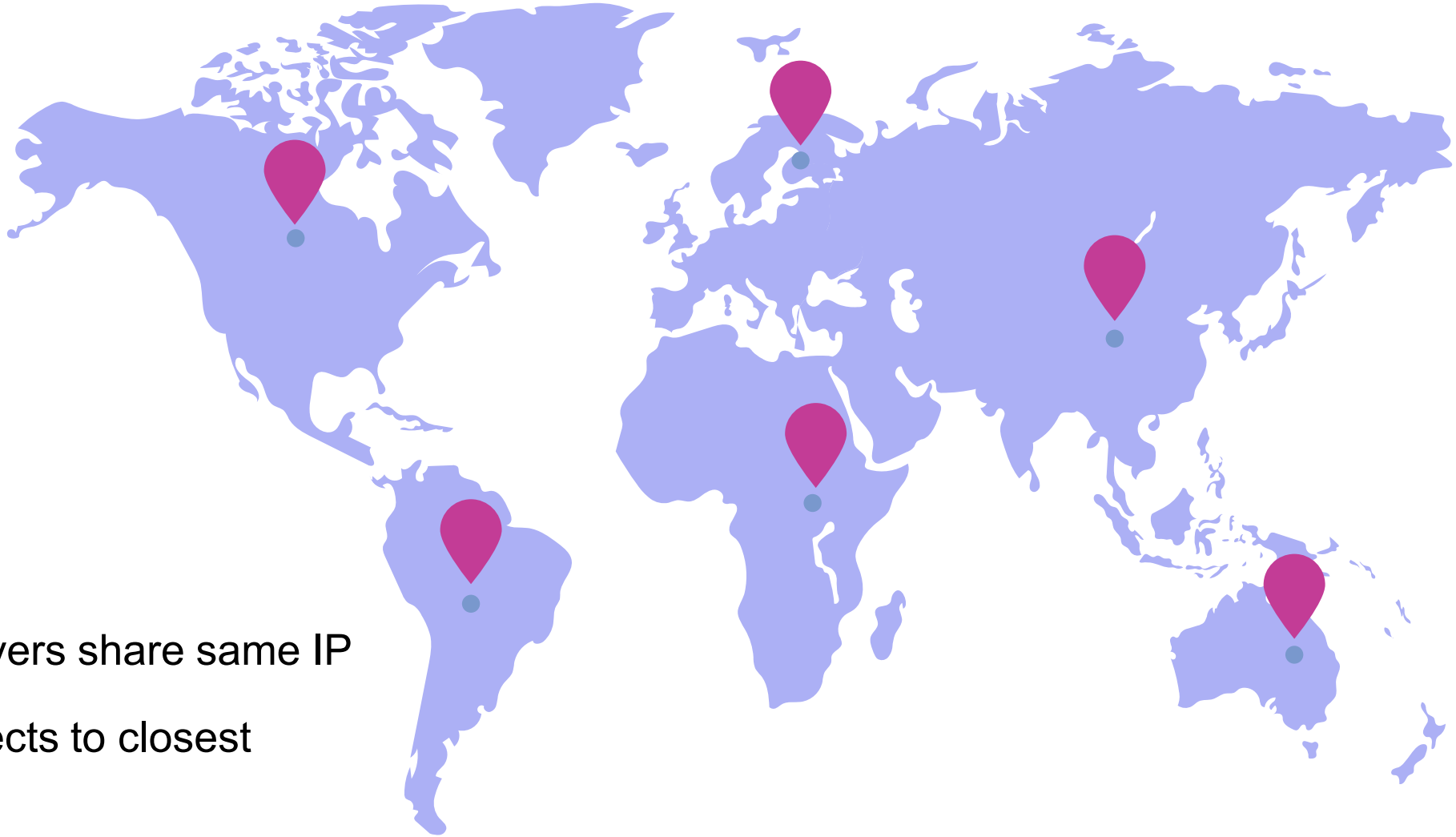


Rate Limiting



Capping number of queries a ‘client’ can make

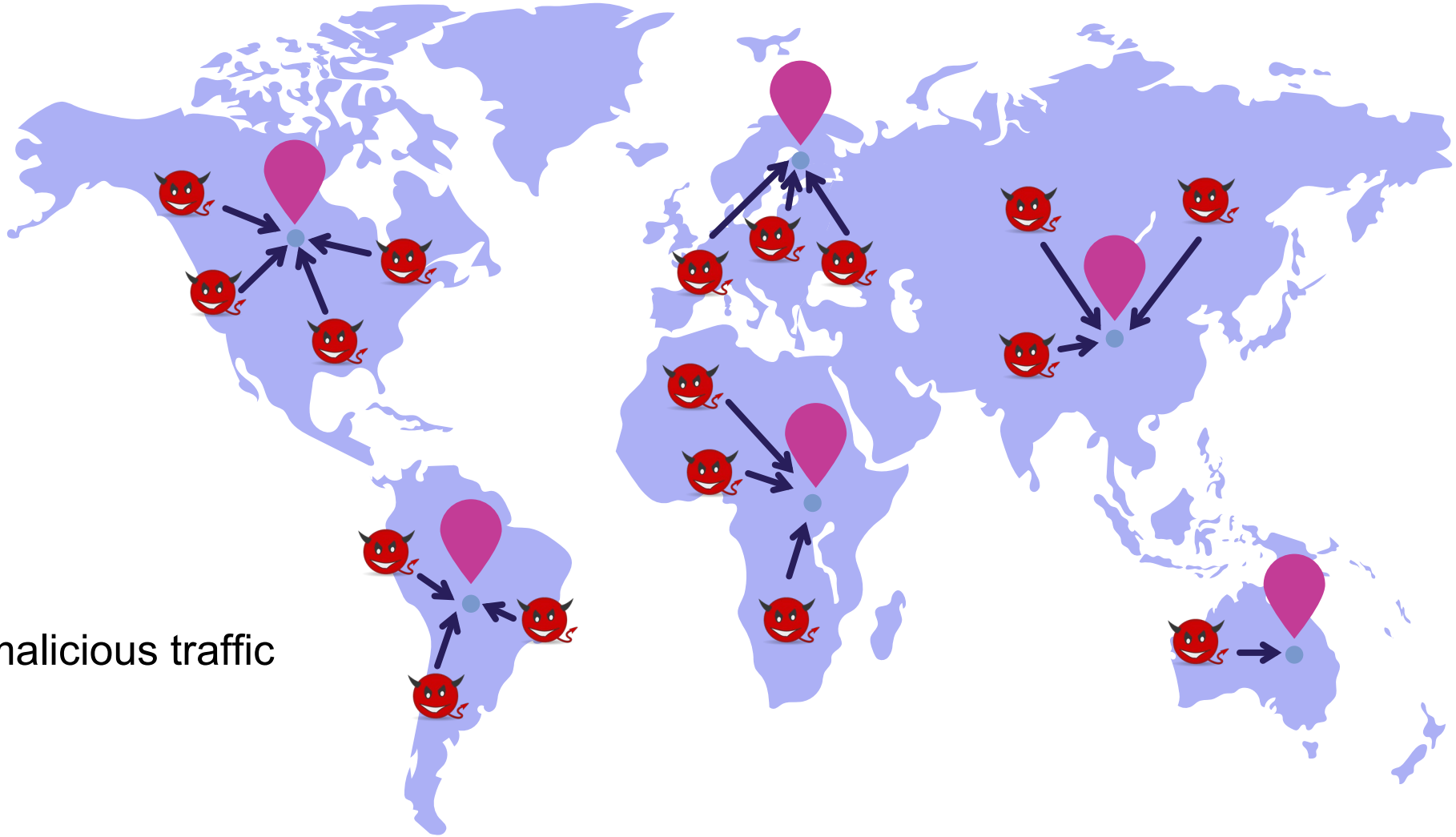
Anycast DNS



Multiple servers share same IP

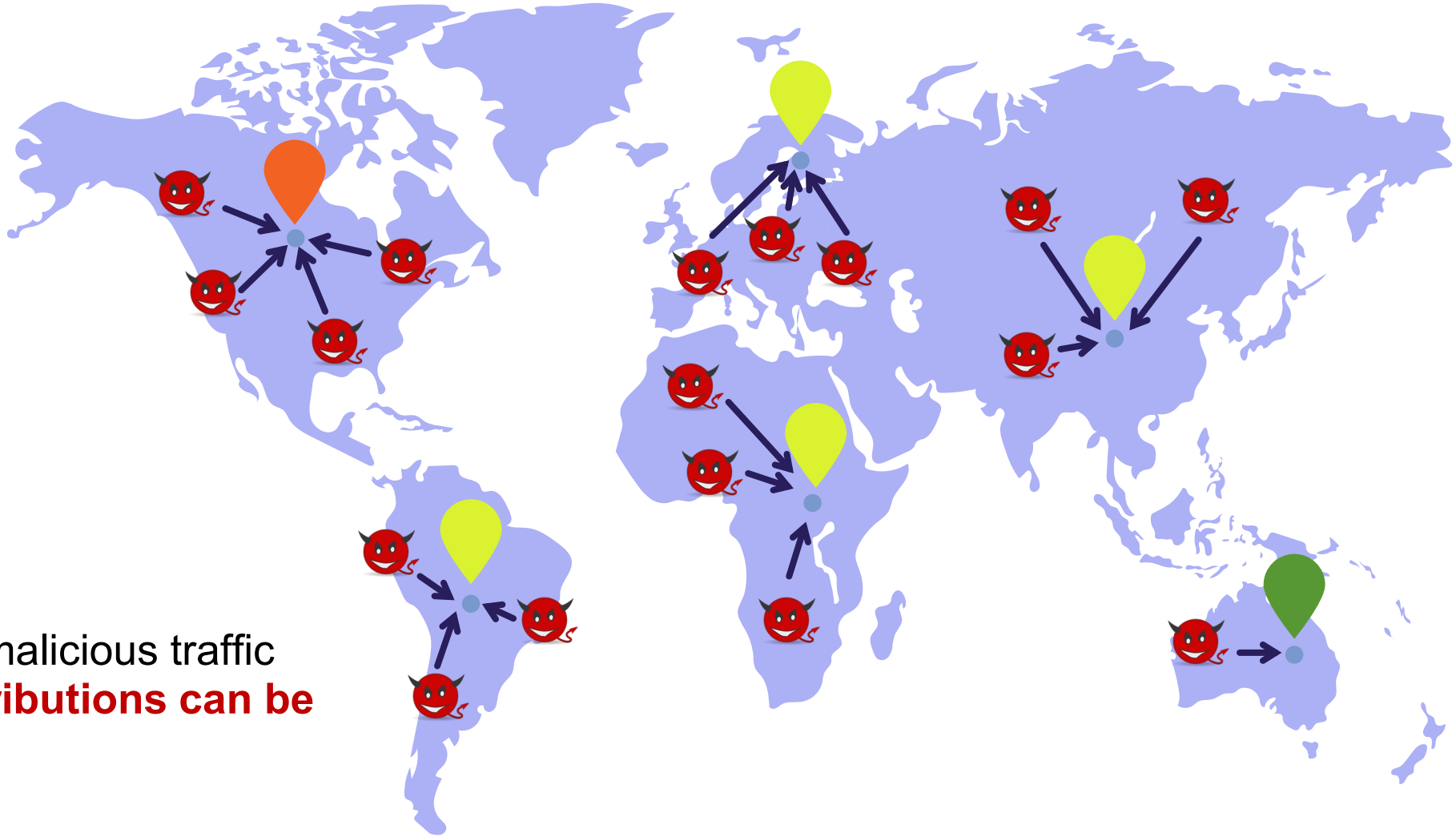
Client connects to closest

Anycast DNS



Distributes malicious traffic

Anycast DNS



Distributes malicious traffic
Traffic distributions can be uneven

Source Authentication

Useful against reflection attacks
Provide meaningful rate limiting & blacklisting

Network Working Group — P. Ferguson
Request for Comments: 2827 — Cisco Systems, Inc.
Obsoletes: 2267 — D. Senie
BCP: 38 — Amaranth Networks Inc.
Category: Best Current Practice — May 2000

Network Ingress Filtering:
Defeating Denial of Service Attacks which employ
IP Source Address Spoofing

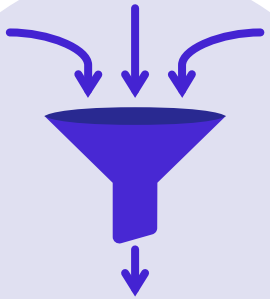
80% deployed

20% permit spoofing [1]

- DNS Cookie
- DNS over HTTPS/QUIC/TLS

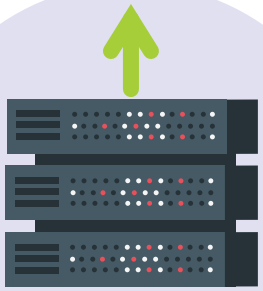
[1] MIT Ana Spoofer Project

Monitoring

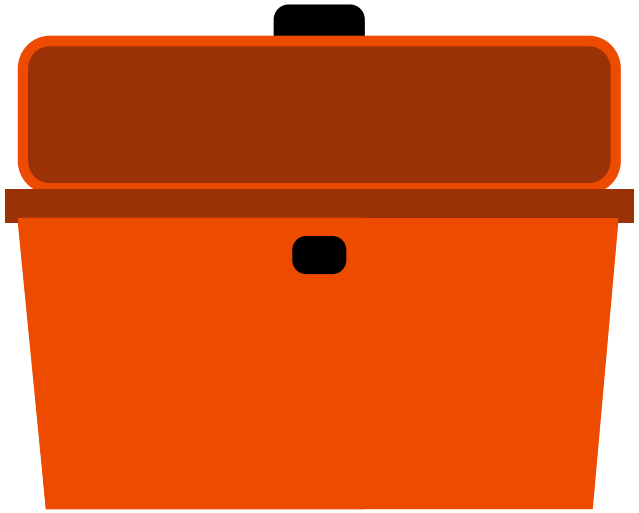


Rate Limiting

Anycast



Overprovisioning



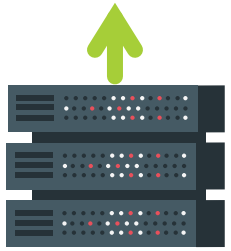
Source Authentication

Enough?

Issues

Monitoring:
Arms race to find new attacks

Issues



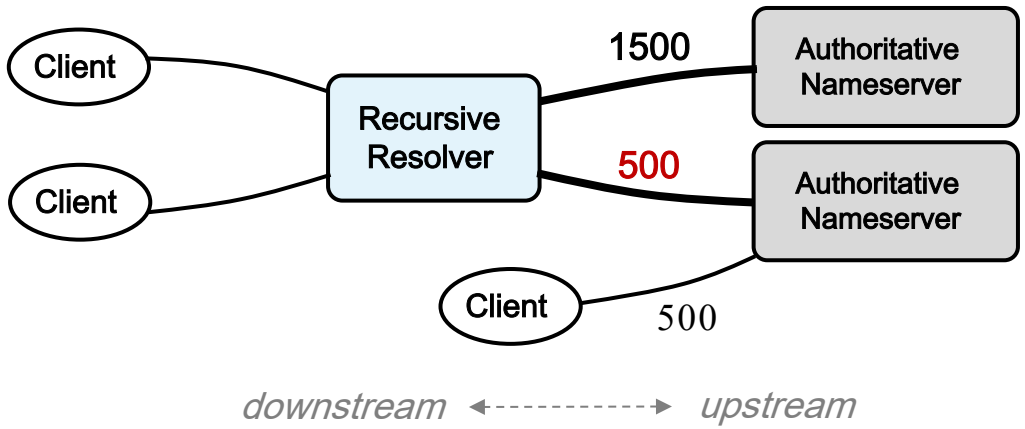
Overprovisioning:

- Effectiveness neutralized by amplification
- Attack traffic can still exhaust resources

Issues

Rate Limiting:

- Attackers can spoof IP addresses to evade rate limit
- Disproportionate impact due to multi-layer structure of DNS



Issues

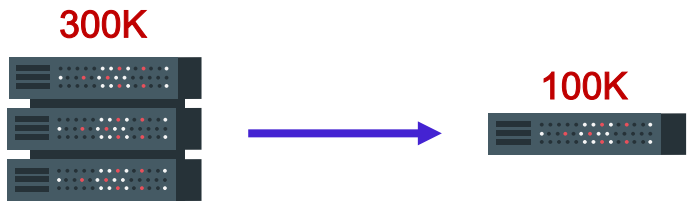
Source Authentication:

- Schemes rely on 1-RTT adding delay
- Secure channels based on public key cryptography (e.g., DoH/DoT/DoQ) are expensive and susceptible to DoS

Issues

Anycast:

- Catchment areas can be imbalanced
- Cascading failure if high-volume location is overwhelmed and switches over to low-volume location



What can we add?
Future defenses

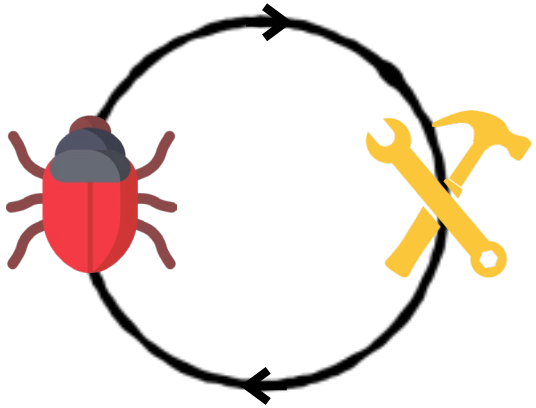
DNS has epic complexity

- Over ***300*** RFCs
- Over ***5000*** pages
- Growing at ***~2 pages / week***
- Features are **entangled**

Natural language introduces **ambiguities**

Need for a proactive approach

Break-and-Fix is insufficient



Automated verification to detect bugs & vulnerabilities

Based on **precisely defined mathematical models**

Our recent DNS formal framework

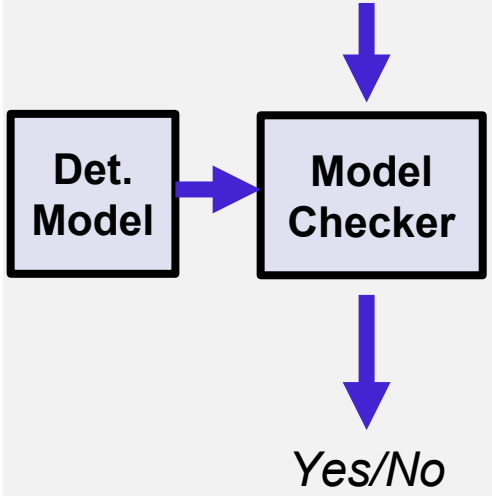
- Comprehensive executable formal semantics for DNS resolution
- Resolve ambiguities whenever possible, otherwise make features configurable

Option	Definition	Default
`rsvMinCredClient`	The minimum credibility requirement [21] for data served to a client	2
`rsvMinCredResolver`	The equivalent credibility requirement for resolver subqueries	2
`maxMinimiseCount`	The MAX_MINIMIZE_COUNT parameter to limit extra work for QMIN [11]	10
`minimiseOneLab`	The MINIMIZE_ONE_LAB parameter from the same mechanism above	4
`rsvTimeout`	Whether and how long a resolver applies a timeout for each query it sends	false, 20.0
`rsvOverallTimeout`	Whether and how long a resolver applies an overall timeout for a client request	false, 100.0

RFC	Description
1034 [36]	Core specification
1035 [37]	Core specification
2181 [21]	Clarifications
2308 [6]	Negative caching
4592 [29]	Wildcards
6604 [25]	RCODE clarifications
6672 [40]	DNAME redirection
8020 [12]	NXDOMAIN clarification
9156 [11]	QNAME minimization

[6] Liu*, Duan*, Heimes, Bearzi, Vieli, Perrig, and Basin, "A Formal Framework for End-to-End DNS Resolution", *SIGCOMM*, 2023

Supports various verification techniques

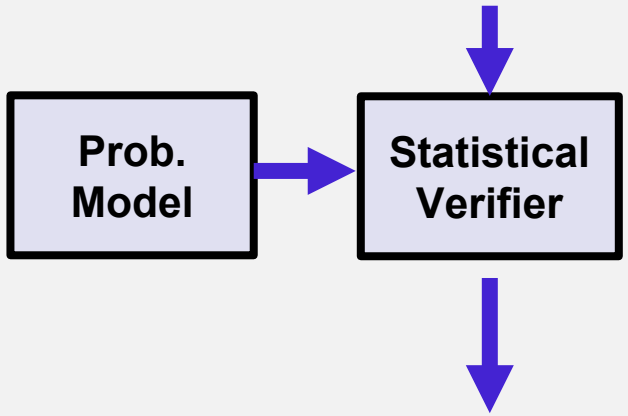


P := absence of

- circular dependency
- answer inconsistency
- rewrite blackhole
- …

Model checking (MC) for **qualitative** properties

What is the **probability** that P holds with a **given statistical confidence**?



P :=

- Query success ratio > 0.9
- Avg query latency < 100 ms
- ...

Statistical MC for **quantitative** properties

Simulation with randomized state generation for **automated** vulnerability analysis
→ **(re-)discovered both known amplification vulnerabilities + new ones**

Formal Verification Outlook

- Proactive Vulnerability Detection
- Improved Protocol Design
- Enhanced Trust

- Exhaustive exploration of DNS resolution state space
- Lots of human effort

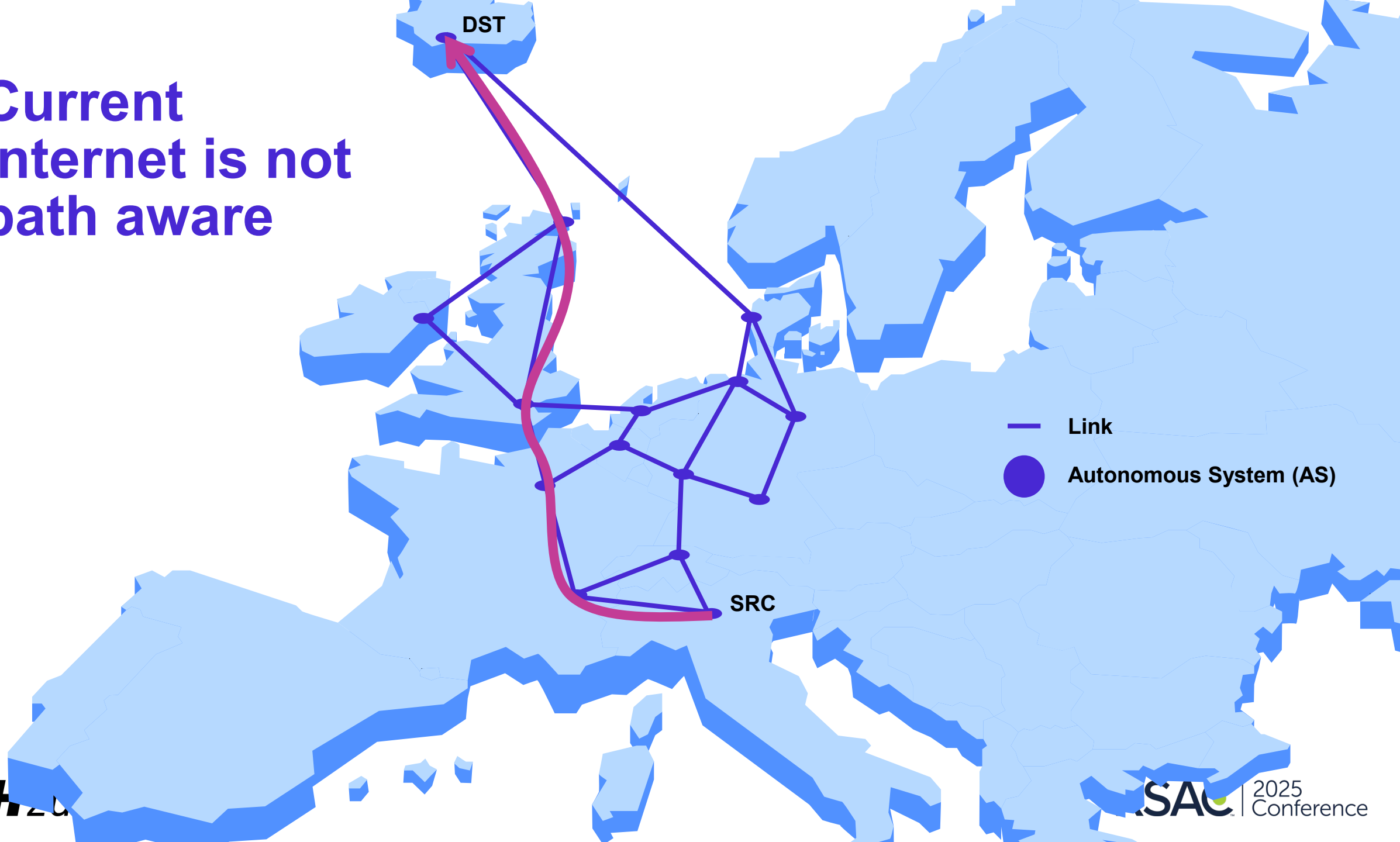
Formal
Verification

Future Internet Architectures

Clean-slate architecture with security in mind

→ Can provide a robust foundation for DNS

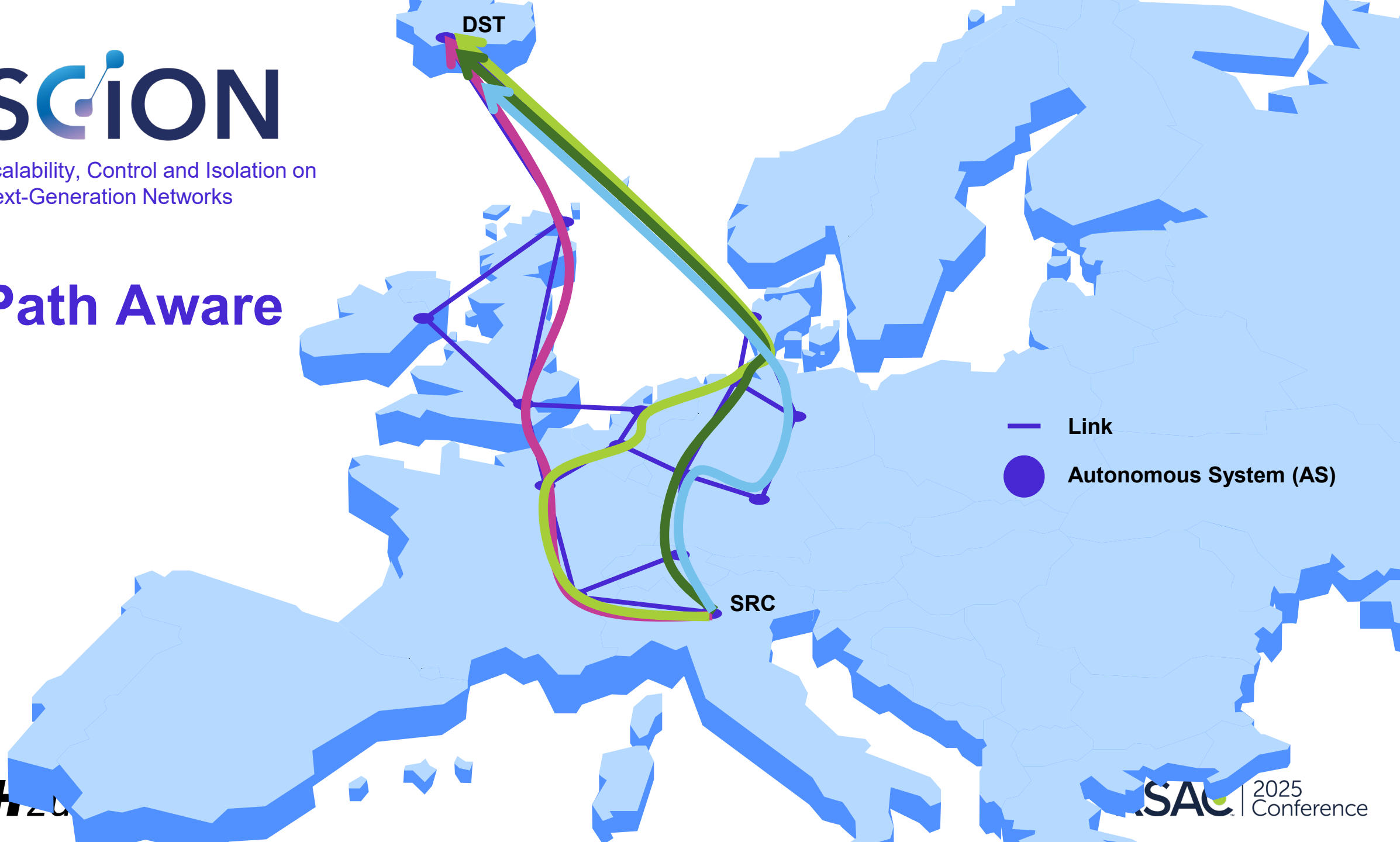
Current Internet is not path aware



SCION

Scalability, Control and Isolation on Next-Generation Networks

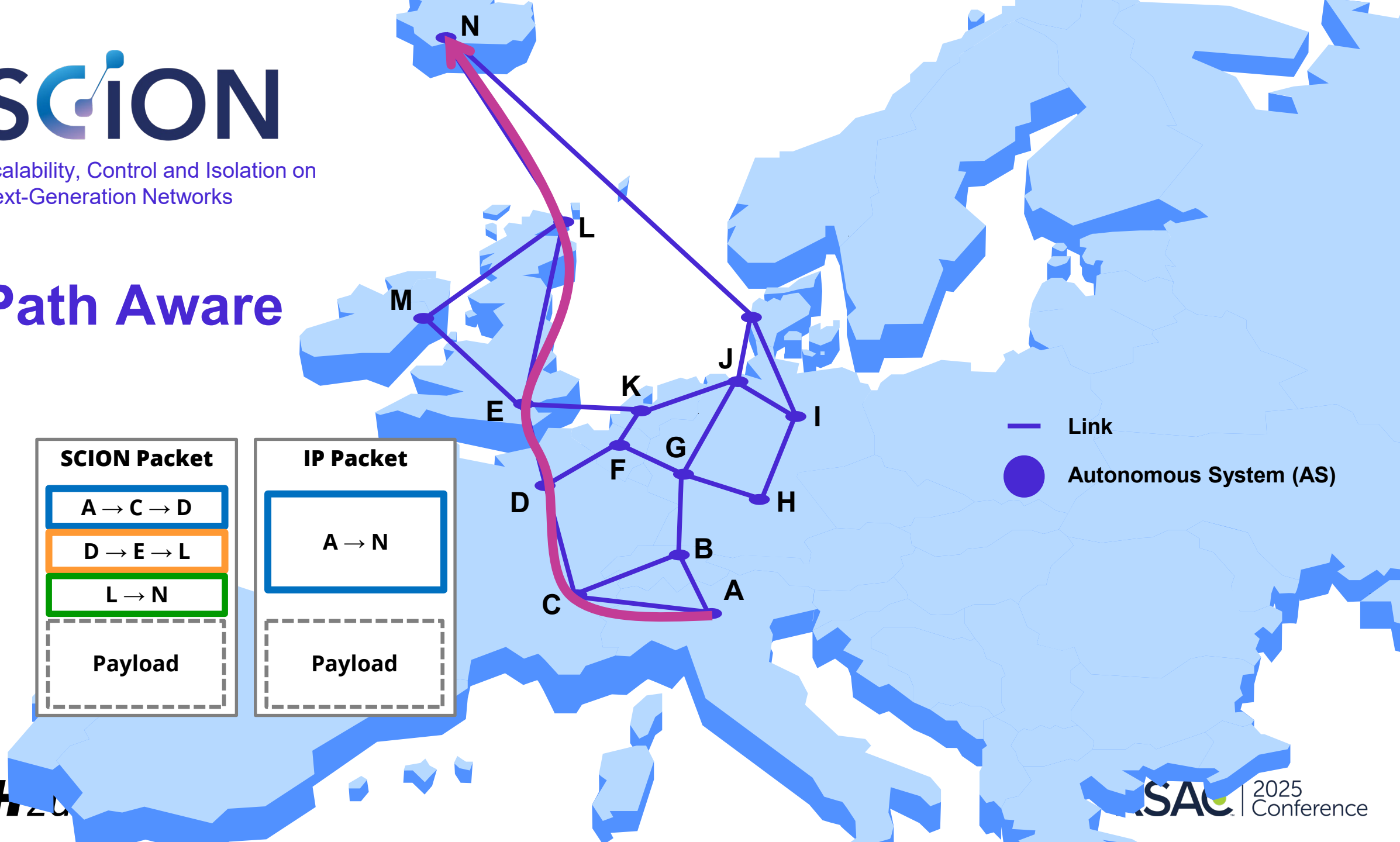
Path Aware



SCION

Scalability, Control and Isolation on Next-Generation Networks

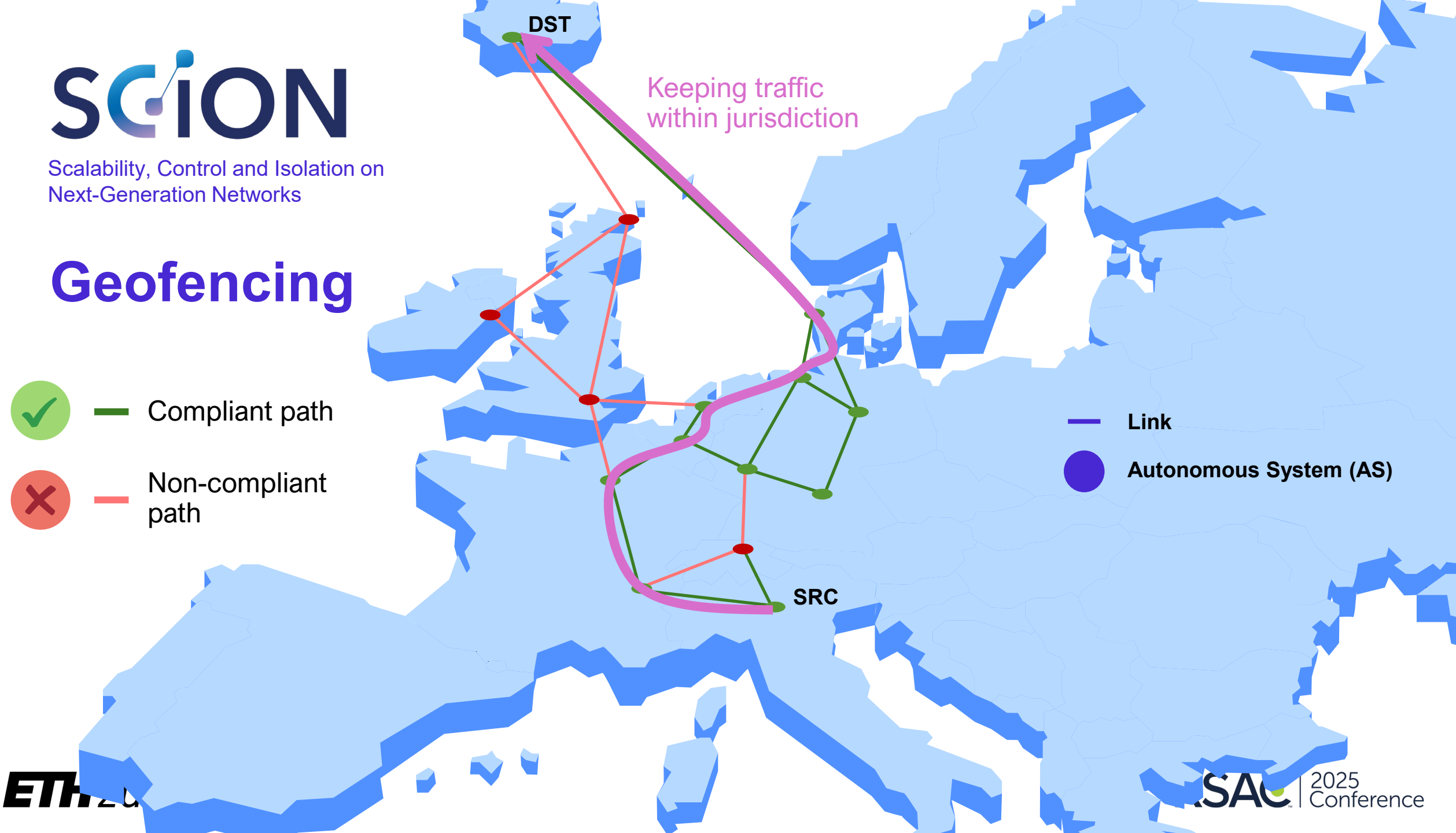
Path Aware



SCION

Scalability, Control and Isolation on Next-Generation Networks

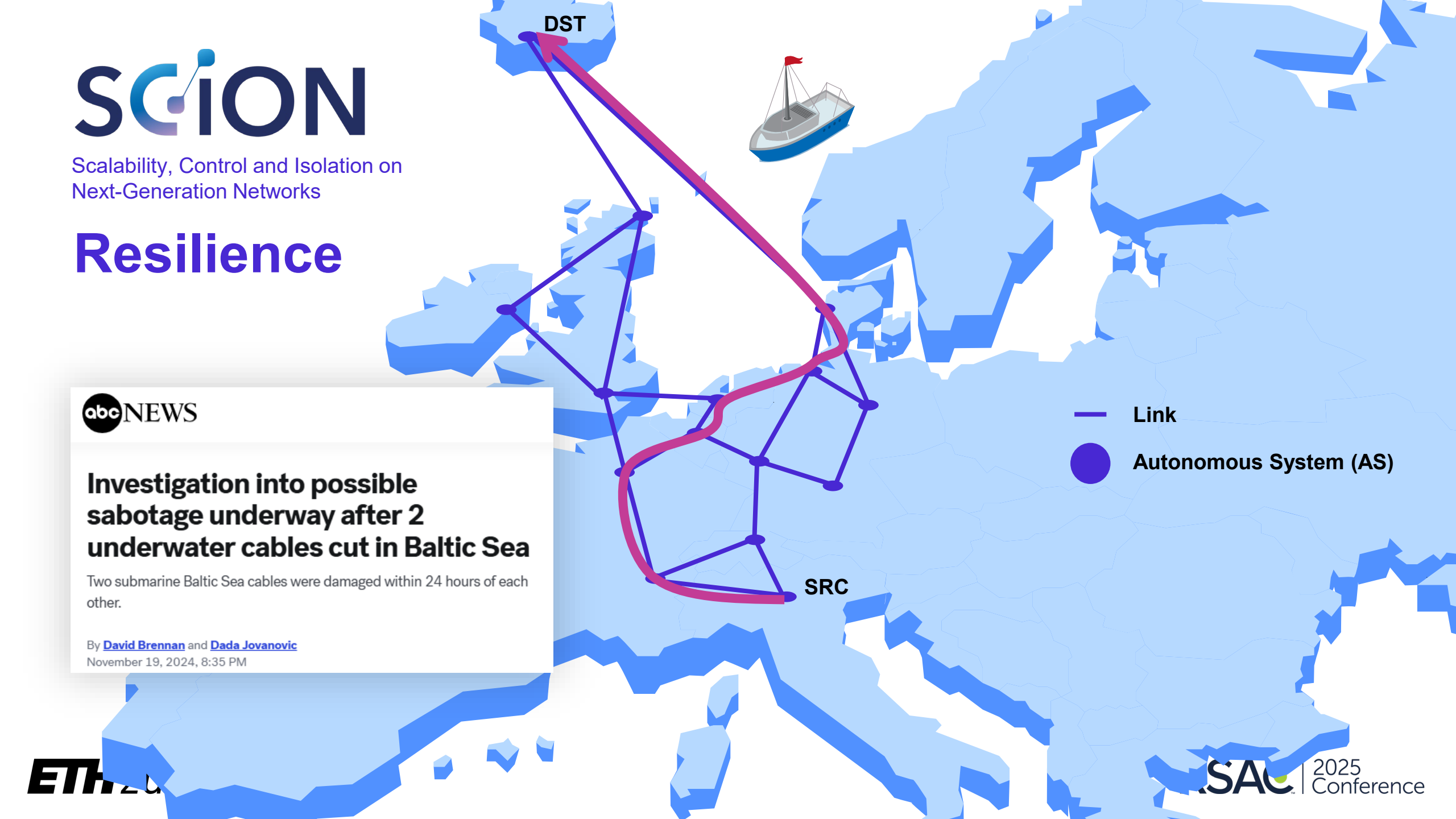
Geofencing



SCION

Scalability, Control and Isolation on Next-Generation Networks

Resilience



abc NEWS

Investigation into possible sabotage underway after 2 underwater cables cut in Baltic Sea

Two submarine Baltic Sea cables were damaged within 24 hours of each other.

By David Brennan and Dada Jovanovic
November 19, 2024, 8:35 PM

SCION

Scalability, Control and Isolation on Next-Generation Networks

Resilience

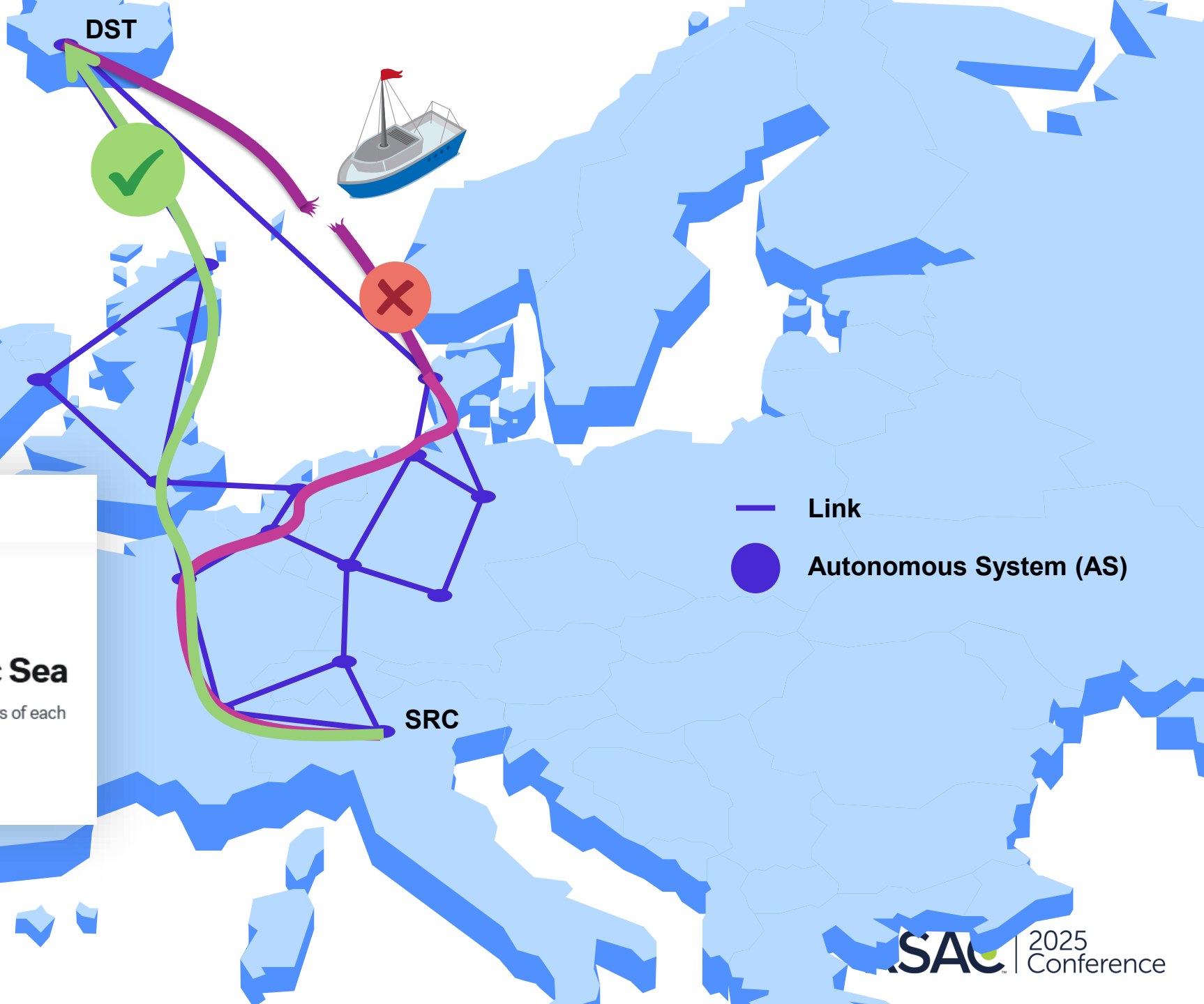
Rapid Failover within RTT magnitude

abc NEWS

Investigation into possible sabotage underway after 2 underwater cables cut in Baltic Sea

Two submarine Baltic Sea cables were damaged within 24 hours of each other.

By David Brennan and Dada Jovanovic
November 19, 2024, 8:35 PM



Resilience against routing failures

Cloudflare 1.1.1.1 incident on June 27, 2024

2024-07-04

Bryton Herdes Mingwei Zhang Tanner Ryan

How Verizon and a BGP Optimizer Knocked Large Parts of the Internet Offline Today

2019-06-24

Tom Strickx

Resilience against routing failures

Cloudflare 1.1.1.1 incident on June 27, 2024

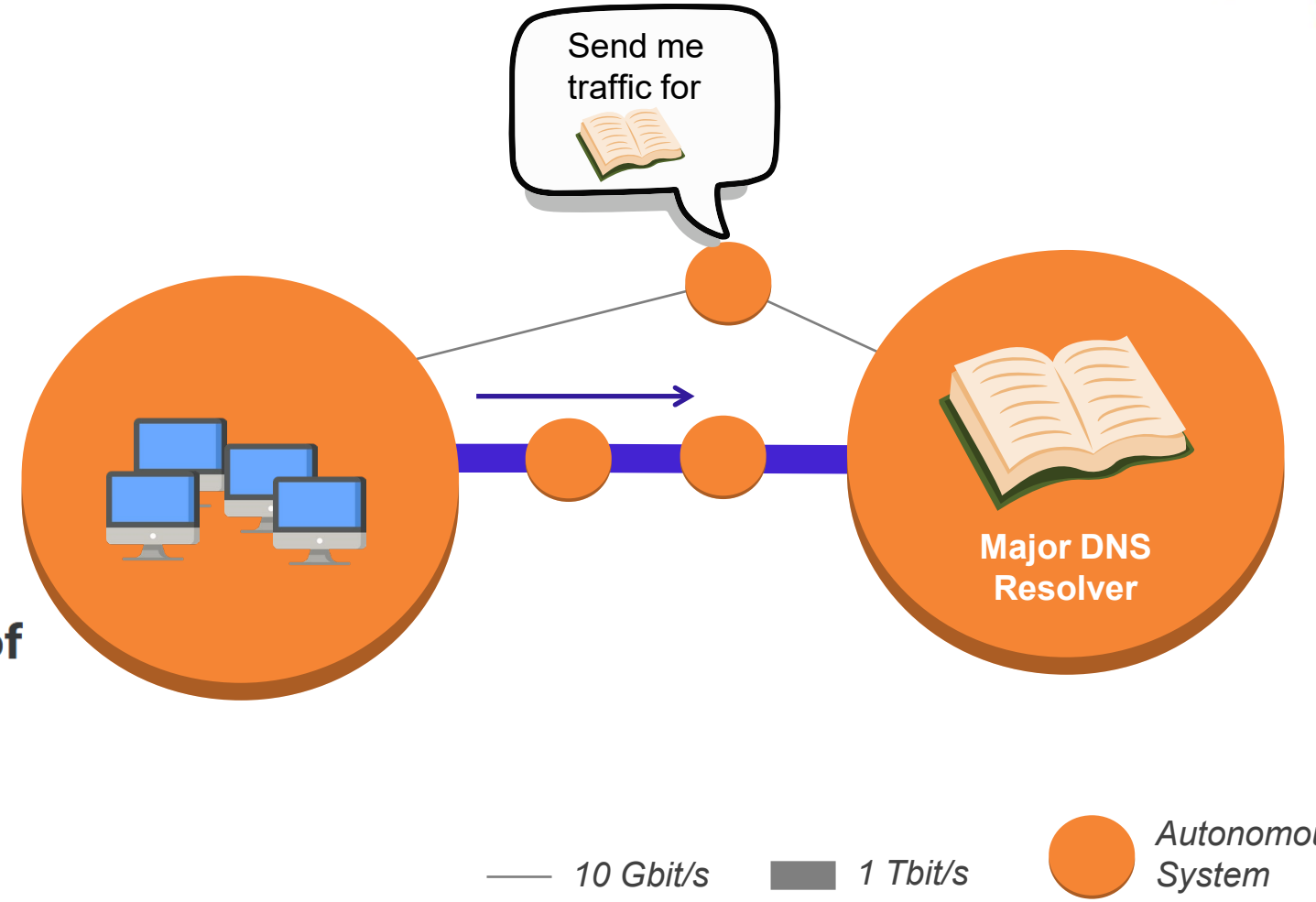
2024-07-04

Bryton Herdes Mingwei Zhang Tanner Ryan

How Verizon and a BGP Optimizer Knocked Large Parts of the Internet Offline Today

2019-06-24

Tom Strickx



Resilience against routing failures

Cloudflare 1.1.1.1 incident on June 27, 2024

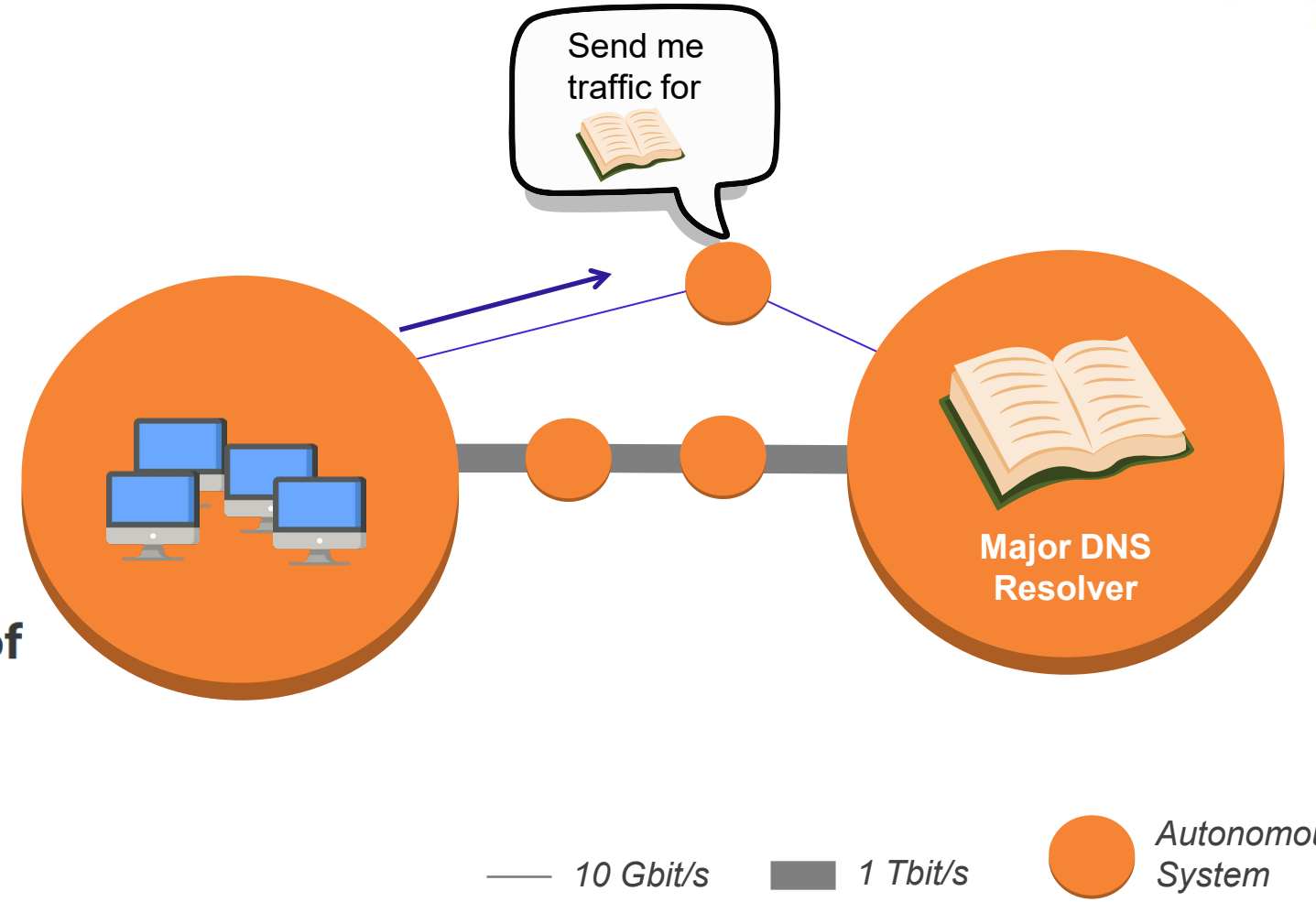
2024-07-04

Bryton Herdes Mingwei Zhang Tanner Ryan

How Verizon and a BGP Optimizer Knocked Large Parts of the Internet Offline Today

2019-06-24

Tom Strickx



Resilience against routing failures

Cloudflare 1.1.1.1 incident on June 27, 2024

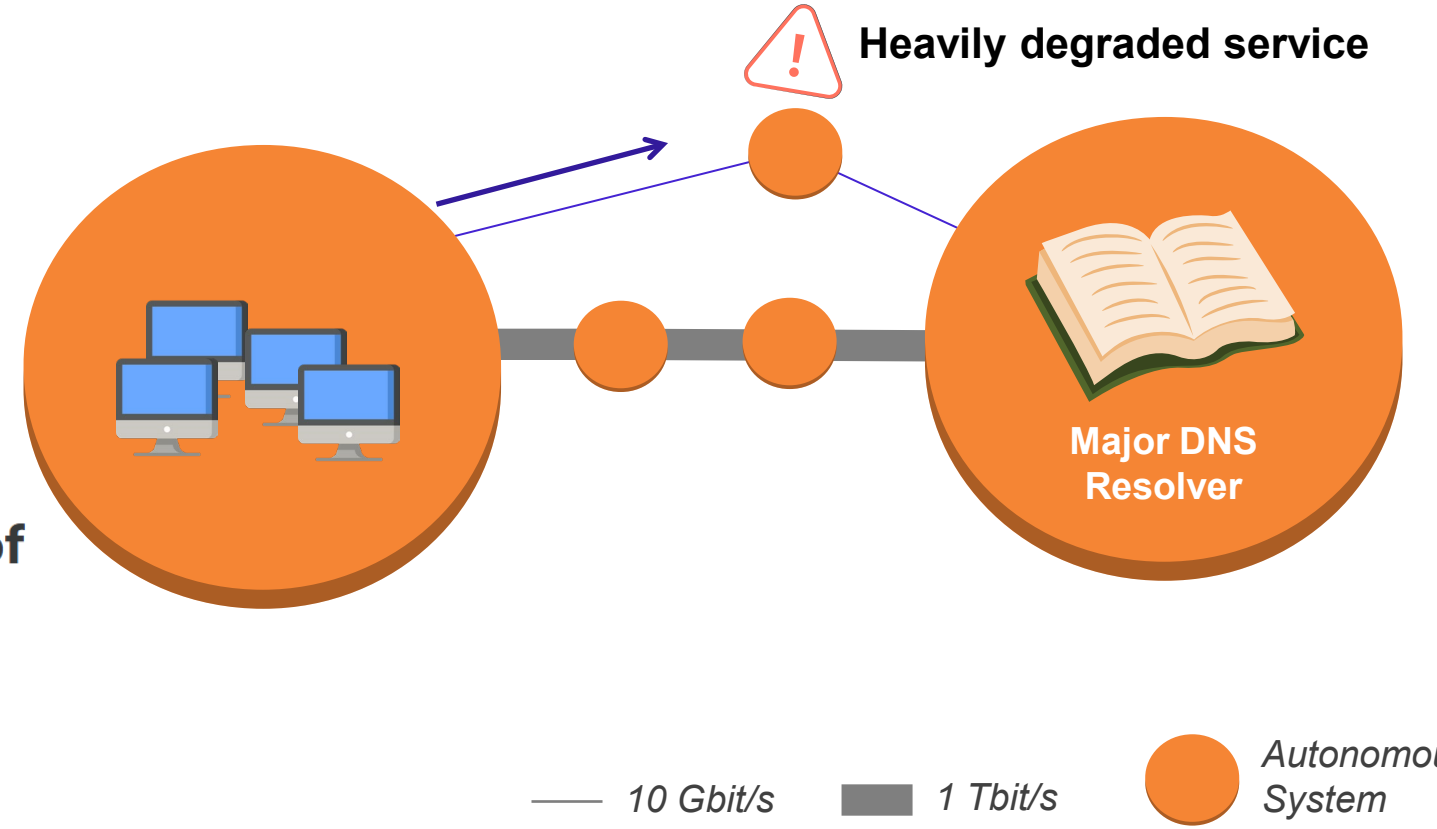
2024-07-04

Bryton Herdes Mingwei Zhang Tanner Ryan

How Verizon and a BGP Optimizer Knocked Large Parts of the Internet Offline Today

2019-06-24

Tom Strickx



* simplified toy example

Other SCION Features

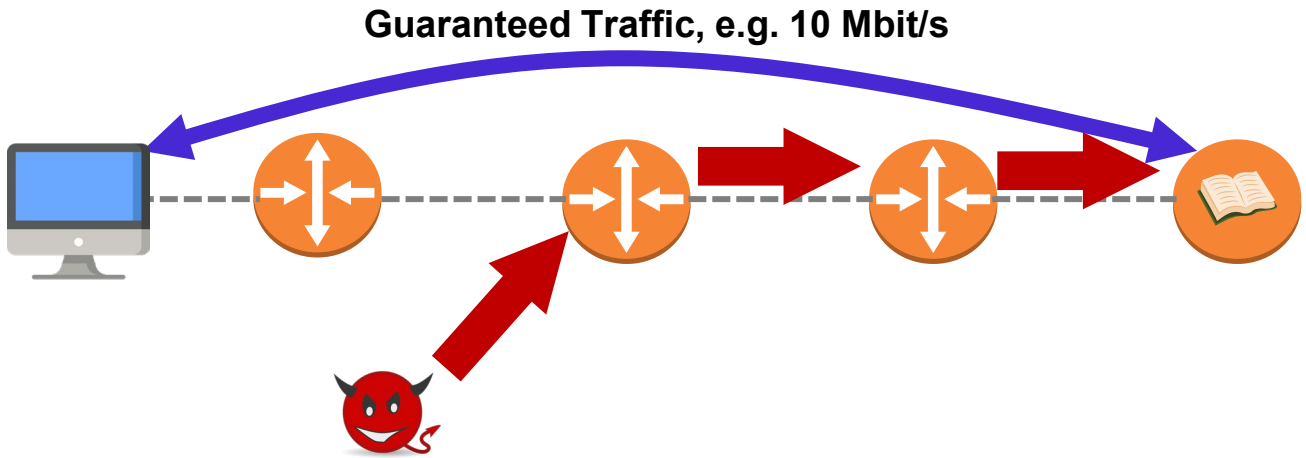
Source Authentication

- Attackers cannot forge sources or manipulate routing
- Source can be validated at first packet, no RTT

For DNS: Meaningful rate limiting + blacklisting, prevent reflection

Legner, Markus, et al. “EPIC: Every Packet Is Checked in the Data Plane of a Path-Aware Internet”. USENIX Security 2020

Bandwidth Reservation



Guarantee that your DNS traffic makes it to the server, like a leased line.

Reserve resources on the DNS server
→ Guaranteed name resolution

SCION Outlook

- Security and reliability guarantees
  - Well-suited for critical infrastructure, such as **DNS**
- Works alongside current internet
- Expanding, with largest deployments in Switzerland
  - **Secure Swiss Finance Network:** 321 participants (banks, insurance companies, securities firms)
  - **Secure Swiss Healthcare Network:** securing 50’000 doctor’s communication
  - **SCION Education, Research and Academic Network**: research institutes across 5 continents

Formal Verification

SCION
Resilience +
BW Reservation
+ Source Auth.

Apply What You Have Learned Today

- Bound resolver work
- Leverage existing toolbox, e.g.
  - Deploy overprovisioning and anycast whenever possible
  - Monitor anomalous queries and block suspicious IPs/domains
- Explore future tools
  - Formal verification
  - SCION-enabled DoS defenses

RSAC | 2025 Conference

Many Voices.
One Community.

Thank you for listening!

Contact us at

netsec.ethz.ch

Dr. Huayi Duan
Jelte van Bommel

Network Security Group
ETH zürich

Acknowledgements
Hasler Stiftung
SNSF
Swiss NCSC